Recibido: 5/10/2020 / Aceptado: 10/11/2020
doi: https://doi.org/10.26439/interfases2020.n013.4876

Modelo Balanced Scorecard para los controles críticos de seguridad informática según el Center for Internet Security (CIS)

William-Rogelio Marchand-Niño
william.marchand@unas.edu.pe / ORCID: 0000-0003-2650-4226

Edwin Jesús Vega Ventocilla
edwin.vega@unas.edu.pe / ORCID: 0000-0002-3628-9016

Universidad Nacional Agraria de la Selva, Tingo María, Perú

Resumen

En diversos sectores de las actividades humanas, las organizaciones están adoptando con mayor intensidad las tecnologías de la información (TI). De este modo, exponen datos sensibles y confidenciales de empleados y clientes, lo cual genera que las entidades públicas y privadas desarrollen normas y regulaciones para proteger estos activos y asegurar su confidencialidad, integridad y disponibilidad. Como resultado del estudio, se formula un modelo de Cuadro de Mando Integral que vincula a los controles críticos de seguridad del CIS, soportado además por un aplicativo de ofimática como una herramienta preliminar que facilite la presentación de resultados. Dichos resultados resaltan que sobre la aplicación preliminar que se dio en cinco instituciones, la mayor proporción (80 %) está de acuerdo con el modelo propuesto y su utilidad para el monitoreo y gestión de los controles de seguridad.

PALABRAS CLAVE: cumplimiento / seguridad y privacidad / modelamiento organizacional

Abstract

BALANCED SCORECARD MODEL FOR CRITICAL COMPUTER SECURITY CONTROLS ACCORDING TO THE CENTER FOR INTERNET SECURITY (CIS)

In different sectors of human activities, organizations are adopting information technology (IT) more intensively, exposing sensitive and confidential information of employees and customers. This situation makes public and private entities to develop standards and regulations to protect these information assets, ensuring confidentiality, integrity and availability. As a result of the study, a Balanced Scorecard model that links the critical security controls of the CIS is formulated and supported by an office IT application as a preliminary tool that facilitates the presentation of the results. Such results highlight that the highest proportion (80%) of the preliminary application that occurred in five institutions agrees with the proposed model and its usefulness for monitoring and managing security controls.

KEYWORDS: compliance / security and privacy / organizational modeling

1. INTRODUCCIÓN

El hecho de que las organizaciones estén adoptando con más intensidad las tecnologías de la información (TI) y aspectos de seguridad, se está convirtiendo en algo más relevante porque se expone información sensible y personal en las soluciones tecnológicas como sitios web, aplicaciones de escritorio, aplicaciones web, aplicaciones móviles, y aplicaciones para internet de las cosas (IoT). Del mismo modo, las regulaciones gubernamentales y estándares relacionados se han estado desarrollando, quizá no a la velocidad del desarrollo tecnológico, pero sí tratando de cubrir la mayor parte de aspectos como el financiero, salud, contable, datos personales, etcétera. Sobre esto mencionan por ejemplo que en Estados Unidos se tiene la Ley SOX para prevenir fraudes contables y financieros incluyendo los registros que son creados y mantenidos con TI (Herath, T., Herath, H. y Bremser., 2010), la Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPPA) para información relacionada a la salud de las personas y otras regulaciones internacionales como International Financial Reporting Standards (IRFS). Asimismo, el sector bancario cuenta con el Payment Card Industry Data Security Standard (PCI DSS) (PCI Security Standards Council, 2016) para la administración de tarjetas de crédito. También los conocidos estándares de la familia ISO/IEC 27000 y de NIST (National Institute of Standards and Technology).

Una de las dificultades de estos estándares y regulaciones es el número y diversidad de controles que contienen; por ejemplo, la familia ISO/IEC 27000 (ISO/IEC, 2013) que define 114 controles, el NIST (National Institute of Standards and Technology, 2014) que define 444 controles de seguridad. Y en un intento de resumirlos, el Centro para la Seguridad de Internet (CIS, 2018) (CIS, Center for Internet Security) ha establecido los veinte controles críticos de seguridad. Asimismo, mantiene manuales denominados CIS Benchmarks orientados a plataformas específicas como sistemas operativos, dispositivos de red, motores de bases de datos, entre otros, cuyo volumen de controles e indicadores pueden superar fácilmente la centena.

Considerando la cantidad de controles que se deben aplicar y evaluar, además de las exigencias por las regulaciones o estándares, las organizaciones están frente a la tarea complicada de realizar el seguimiento, monitoreo y evaluación de los controles de seguridad de forma efectiva y eficiente.

Ante ese escenario, realizar un adecuado seguimiento y control de los indicadores de seguridad definidos en una organización es sumamente importante, sea por cumplimiento regulatorio o no. Por otro lado, hay propuestas de Balanced Scorecard (BSC) para seguridad informática, como la propuesta por DeLooze (2006), bajo los mismos principios del BSC tradicional como aquella que define cuatro grupos de *stakeholders* para un programa de seguridad y su aseguramiento. Los cuatro grupos propuestos son: usuarios, administradores, administradores de sistemas o dueños de los sistemas, y los

auditores o reguladores (DeLooze, 2006). Según el autor de la mencionada propuesta, el enfoque propuesto permite responder preguntas del tipo "¿cómo ve nuestro programa de seguridad a nuestros usuarios?", "¿cómo ve nuestro programa de seguridad a los propietarios del sistema?", "¿cómo ve nuestro programa de seguridad a nuestros administradores de sistemas? y "¿cómo ve nuestro programa de seguridad a los auditores?".

La adaptación de un modelo de BSC para seguridad de la información también fue abordada por algunos autores, quienes le dan un enfoque estratégico a la seguridad afirmando, por ejemplo, que uno de los aspectos importantes respecto a la perspectiva de valor para el negocio es proteger la reputación y generar confianza. Y esto se puede lograr con una efectiva aplicación de controles y el seguimiento a estos (Groš, 2019). Para efectos de esta investigación se consideran los controles CIS por la disponibilidad de la documentación detallada de forma libre, además de una oportunidad de profundizar el análisis de la aplicación de estos controles y sus beneficios. Por lo tanto, la pregunta de investigación se define de la siguiente manera: ¿de qué forma el Cuadro de Mando Integral se adecúa para el monitoreo del cumplimiento de los veinte controles críticos de seguridad del Center for Internet Security? El objetivo es, por lo tanto, determinar la manera en que el Cuadro de Mando Integral constituye una plataforma apropiada para el monitoreo del cumplimiento de los veinte controles críticos de seguridad propuestos por el CIS.

La hipótesis sobre la cual gira la investigación está formulada del siguiente modo: "Un modelo de Balanced Scorecard para seguridad informática ofrece una estructura de monitoreo efectivo y eficiente al cumplimiento de los veinte controles críticos de seguridad del Center for Internet Security". La investigación se justifica técnicamente porque se aplicarán conceptos sobre controles de seguridad informática y el Cuadro de Mando Integral (Balanced Scorecard). Desde el punto de vista organizacional, la investigación proporciona una herramienta a nivel estratégico para el monitoreo de los controles de seguridad informática que se deben implementar por exigencias regulatorias o por política institucional. La principal característica y contribución de esta investigación es la de ofrecer una alternativa que integre las mediciones operativas con la herramienta de gestión estratégica en términos de seguridad.

El artículo se compone de seis secciones siendo esta introducción la primera de ellas. En la sección 2 se realiza la revisión de la literatura que considera los principales antecedentes y principios. En la sección 3 se detalla la metodología para la construcción de la propuesta del modelo de BSC adaptada al monitoreo de los controles CIS, mientras que la sección 4 está dedicada a la presentación y discusión de los resultados obtenidos en la fase de evaluación. En la sección 5 se brindan las conclusiones del trabajo y, finalmente, en la sección 6 se describen las posibles líneas de trabajo futuro.

2. REVISIÓN DE LITERATURA

2.1 Cuadro de Mando Integral (Balanced Scorecard)

El Balanced Scorecard o Cuadro de Mando Integral (CMI), desarrollado por Kaplan y Norton en 1992, es más que solo un instrumento de medición. Es un sistema de gestión estratégica con una visibilidad y comprensión de los objetivos y métodos para alcanzarlos. Esto implica que se deben traducir en indicadores que reflejen la evaluación del desempeño de las estrategias implementadas (R. Kaplan y Norton, 2002, R. S. Kaplan y Norton, 2005).

El Cuadro de Mando Integral (CMI) orienta su uso a la alineación de indicadores financieros y no financieros para la gestión y control del rendimiento de las organizaciones (Caudle, 2008, R. S. Kaplan y Norton, 1996). Además, el CMI está pensado para la gestión de las estrategias formuladas en un plan estratégico institucional y el soporte para la materialización de los inductores y acciones que lo contienen (Marchand-Niño, 2013). En la figura 1 se pueden observar las cuatro perspectivas clásicas del CMI: financiera, cliente, procesos internos y la perspectiva de aprendizaje y crecimiento.

La evolución de los procesos en las organizaciones hace que se adopten las tecnologías de la información (TI) que suman complejidad, y la necesidad de desarrollar nuevos enfoques para el seguimiento y control del rendimiento organizacional. Sin embargo, el CMI también resulta útil para tales propósitos, es así que se formula un Balanced Scorecard (BSC) adaptado para sistemas de información (SI) (Martinsons, Davison y Tse, 1999). Las perspectivas consideradas en este CMI son orientación al usuario, valor para el negocio, procesos internos y preparación futura (ver figura 2). Como se puede deducir, los sistemas de información son un componente interno, por lo que las perspectivas consideradas en el CMI también son de carácter interno. Sin embargo, no pierde el enfoque estratégico, puesto que los sistemas de información también deben estar alineados a la misión y visión del negocio.

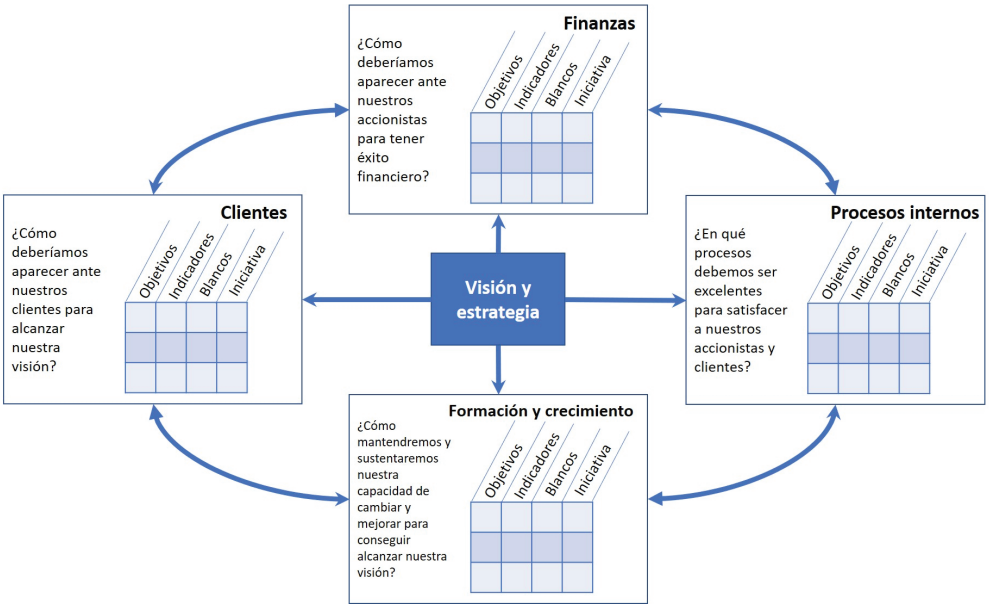

Figura 1. Perspectivas originales del Balanced Scorecard

Fuente: R. Kaplan y Norton, 2002

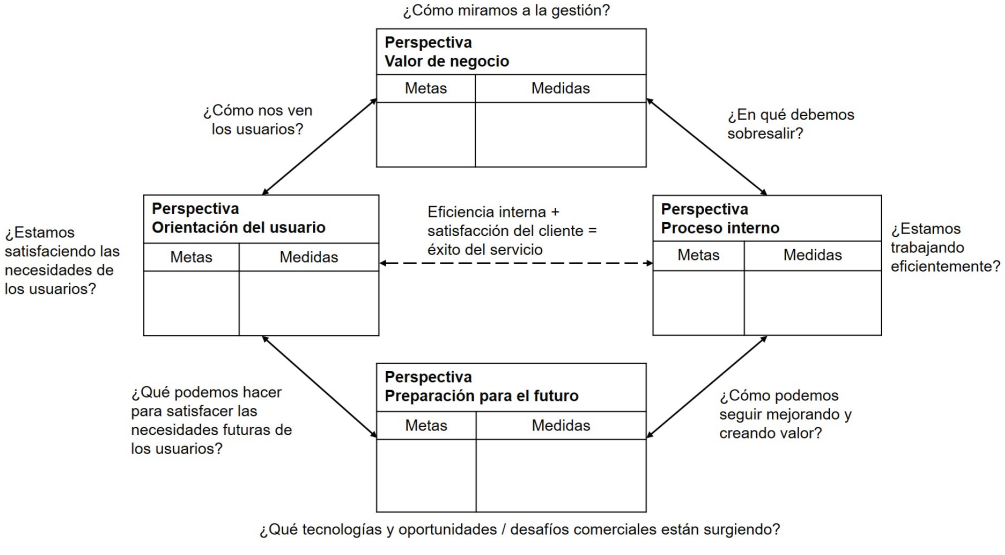

Figura 2. Perspectivas del Balanced Scorecard para sistemas de información

Fuente: Martinsons, Davison y Tse, 1999

Los administradores de TI buscan herramientas que les faciliten alinear los recursos de las tecnologías de información con el negocio y realizar un control de cómo estos contribuyen al soporte y rendimiento de la organización (Keyes, 2005). Una de esas herramientas de alto valor es el Cuadro de Mando Integral que debe poseer los atributos, como sencillez de presentación, enlaces explícitos a la estrategia de TI, amplio compromiso ejecutivo, definiciones de métricas estándar de empresa, capacidad de desglose y contexto disponible. Además, las métricas que se deben considerar se agrupan en siete categorías: rendimiento financiero, rendimiento del proyecto, rendimiento operacional, gestión del talento, satisfacción del usuario, iniciativas empresariales y seguridad de la información. Se evidencia que las métricas relacionadas con la seguridad de la información hacen su aparición en estos tipos de Balanced Scorecard.

Otro trabajo importante que propone un CMI para TI es el desarrollado con perspectivas consideradas que son similares a las de Martinsons (1999), tal como se muestran en la figura 3. Estas perspectivas son: orientación al usuario, excelencia operacional, contribución empresarial y orientación al futuro (Grembergen, 2005).

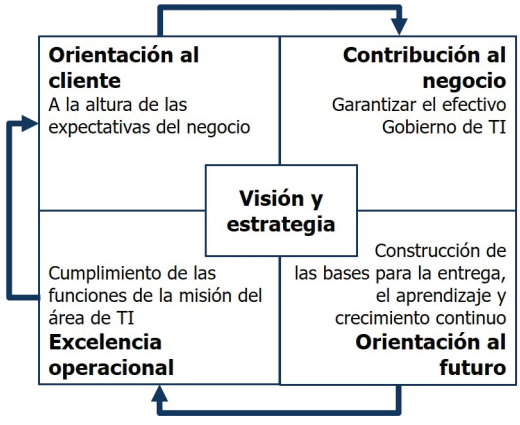

Figura 3. BSC para TI

Fuente: Grembergen, 2005

Como se puede observar en la figura 3, la adaptación de Grembergen (2005) establece la correspondencia con las cuatro perspectivas originales, considerando, además, que el componente de TI es interno en una organización y desde esa visión la perspectiva financiera pasa a conceptuarse como el aporte que realizan las tecnologías de la información al negocio en términos de eficiencia que pueden repercutir en aspectos financieros (ahorros, optimización de costos, etc.); la perspectiva original del cliente se transforma en perspectiva hacia el usuario de las TI. La perspectiva de procesos

internos se orienta a la excelencia operacional en el sentido de cómo las tecnologías de la información soportan el cumplimiento de las funciones del área de TI alineadas a los objetivos estratégicos de la organización; y finalmente la perspectiva de aprendizaje y crecimiento denominada en el BSC para TI como orientación al futuro es un concepto que para abordar las acciones de aprendizaje continuo de acuerdo con el crecimiento y madurez organizacional.

2.2 Controles de seguridad

Para efectos de la investigación, los conceptos y teoría están asociados a la seguridad de la información y seguridad informática.

El NIST en su publicación especial 800-53, define que un control de seguridad es una "salvaguarda o contramedida para proteger la confidencialidad, integridad y disponibilidad de la información de las organizaciones" (National Institute of Standards and Technology, 2014) functions, image, and reputation. Estos controles son necesarios para satisfacer los requerimientos de seguridad definidos por las entidades con el fin de mitigar los riesgos asociados a los activos de información. Definición parecida la realiza el Committee on National Security Systems (CNSS), una fuente autorizada de definiciones en los Estados Unidos que establece como controles de seguridad a aquellos "controles de gestión, operativos y técnicos (es decir, salvaguardas o contramedidas) prescritos para un sistema de información para proteger la confidencialidad, integridad y disponibilidad del sistema y su información" (CNSS, 2015).

Aunque en textos de otros estándares no se describe explícitamente el concepto de control de seguridad, la acepción definida por el CNSS será la que predomine en el desarrollo del proceso de investigación; además es útil ampliar el concepto en el sentido que detallar si existe alguna clasificación para los controles de seguridad y cuáles son las fuentes de datos para realizar el seguimiento o monitorización.

Los controles de seguridad se pueden clasificar en tres tipos:

- **Controles de administración**, acciones tomadas para administrar el desarrollo, mantenimiento y uso de los sistemas; por ejemplo, políticas y procedimientos.
- **Controles operativos**, mecanismos y procedimientos cotidianos utilizados para proteger los sistemas operacionales y su entorno; por ejemplo, formación de conciencia, la gestión de la configuración y la respuesta a incidentes.
- **Controles técnicos**, controles de *hardware / software* utilizados para proteger los sistemas de TI y la información que se almacena, procesa o transmite. Por ejemplo, los controles de acceso, los mecanismos de autenticación y el cifrado (Johnson, 2015).

La cantidad de controles definidos por diversos estándares y entidades reguladoras en el mundo puede convertirse en un problema para la implementación o adopción por las organizaciones, tal es así por ejemplo, que la basada en la ISO/IEC 27001:2013 (Indecopi, 2014) incluye 114 controles agrupados en 35 objetivos de control y 14 dominios, la norma NIST 800-53 revisión 4 (National Institute of Standards and Technology, 2014) establece 444 controles agrupados en 18 familias y el Centro para la Seguridad de Internet (CIS, Center for Internet Security) define los 20 controles críticos de seguridad con 171 subcontroles. Tomando en cuenta el artículo *SIEM-based framework for security controls automation* (Montesino, Fenz y Baluja, 2012), que postula la posibilidad de automatizar algunos controles, se puede facilitar su evaluación. Estos controles de seguridad susceptibles de automatizar son:

- Inventario de activos (*hardware* y *software*)
- Gestión de cuentas
- Gestión de *logs*
- Monitoreo de sistemas
- Protección contra *malware*
- Gestión de actualizaciones y escaneo de vulnerabilidades
- Verificación del cumplimiento y evaluación de seguridad
- *Backup* de información
- Seguridad física
- Gestión de incidentes

Entiéndase por "automatizar controles" al uso de herramientas que permitan recopilar datos en tiempo real o diferido con intervención humana mínima; herramientas como IDS/IPS, sensores, *sniffers*, *software* especializado, SIEM como le desarrollado por Splunk (Splunk Enterprise Security) (Splunk, 2020) o el desarrollado por IBM (IBM QRadar) (IBM, 2020), o como las herramientas *open source,* como el *framework* OSSIM (Our Open Source SIEM) (AT&T Cybersecurity, 2020).

Asimismo, se definen las evaluaciones de los controles de seguridad como "las pruebas o evaluaciones de los controles de seguridad de gestión, operacionales y técnicos para determinar la medida en que los controles se implementan correctamente, operan según lo previsto, y si realmente están produciendo el resultado deseado con respecto al cumplimiento de los requisitos de seguridad para un sistema de información u organización" (CNSS, 2015).

2.3 Evaluación de controles CIS

Entre algunos trabajos relacionados con la evaluación y monitoreo de los controles críticos de CIS se mencionan los siguientes:

Una forma de automatizar controles de CIS respecto a *firewall* de Palo Alto, en la que se propuso una metodología para diseñar una herramienta que automatizara la verificación de los controles CIS en los dispositivos de red de Palo Alto Networks. Algunos de los resultados son correspondientes al consumo de tiempo para las inspecciones manuales y automatizadas, y la carga de trabajo que eso representa para el personal involucrado en ese tipo de servicios (Perminov, Kosachenko, Konev, y Shelupanov, 2020). Otro factor revelado es sobre la capacidad de rastreo y detección de violaciones de seguridad en estos dispositivos lo que permite un tiempo de respuesta más eficaz.

Otro análisis que se realiza sobre los controles de CIS hace referencia a la existencia de múltiples estándares y modelos de controles para la seguridad de la información como ISO, NIST, entre otros, donde CIS nace como una alternativa más práctica y con un número de controles que sean manejables. Sin embargo, con el tiempo se ha convertido también en una solución parecida a las mencionadas sobre gestión de riesgos, aunque con menos controles, pero presentando un catálogo tal cual las demás soluciones (Groš, 2019). La crítica que se plantea es que el CIS de SANS (SysAdmin Audit, Networking and Security Institute) no se convierta finalmente en una opción más, que se realicen análisis más profundos con el propósito de mejorar este modelo de controles.

2.4 BSC para seguridad de la información

La aplicación adecuada del concepto de Balanced Scorecard puede contribuir a mejorar la gestión orientada a las tecnologías de la información y comunicación otorgando un enfoque estratégico a la seguridad. Uno de los aspectos importantes respecto a la perspectiva de valor para el negocio es el proteger la reputación y generar confianza. La perspectiva de los *stakeholders* se orienta hacia el comportamiento de los empleados que puede repercutir en la seguridad en sí misma así como en las necesidades de seguridad de estos que deben ser cubiertas y controladas (Herath *et al.*, 2010). En la perspectiva de procesos internos, los autores plantean que se deben medir de forma similar a otras aplicaciones de TI, considerando tres procesos generales: (1) la planificación y priorización de iniciativas de seguridad, (2) la implementación de servicios y productos de seguridad y (3) las operaciones y mantenimiento de los servicios de seguridad. Finalmente, en la perspectiva de preparación para el futuro, se afirma que un aspecto importante sería la capacitación continua del personal de seguridad de TI y los usuarios sobre diferentes tipos de amenazas y sus formas de evitarlas. En la figura 4 se muestra el modelo propuesto para seguridad de información.

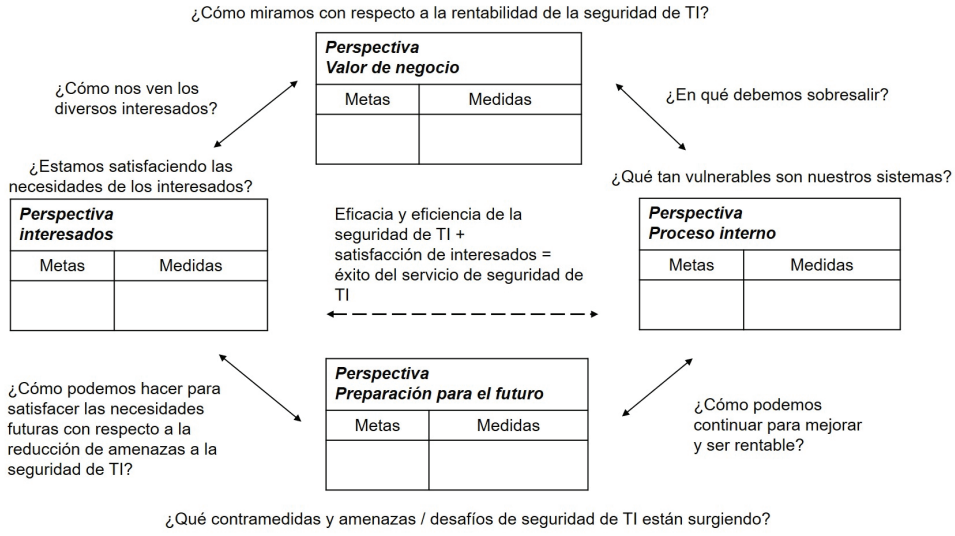

Figura 4. Modelo Balanced Scorecard para seguridad de la información

Fuente: Herath, T., Herath, H. y Bremser, 2010

Una de las preguntas que se formulan en trabajos como el de Herath (2010) es "¿cuáles son las medidas comunes que se utilizan en la seguridad de TI y cómo han cambiado en los últimos años?" Y como parte de una posible respuesta a esa pregunta, este trabajo determinará la forma de incluir los indicadores considerados en estándares difundidos ampliamente en la industria como son los veinte controles del CIS (Center for Internet Security).

3. METODOLOGÍA

En una primera etapa se adaptó el BSC original a un BSC para seguridad informática y posteriormente se realizó un mapeo de los controles del CIS con los cuadrantes del tablero de mando integral.

3.1 BSC para seguridad informática

En esta fase se desarrolla la propuesta del tablero de mando integral (BSC) para seguridad informática, en la cual se considera la analogía presentada en la figura 5.

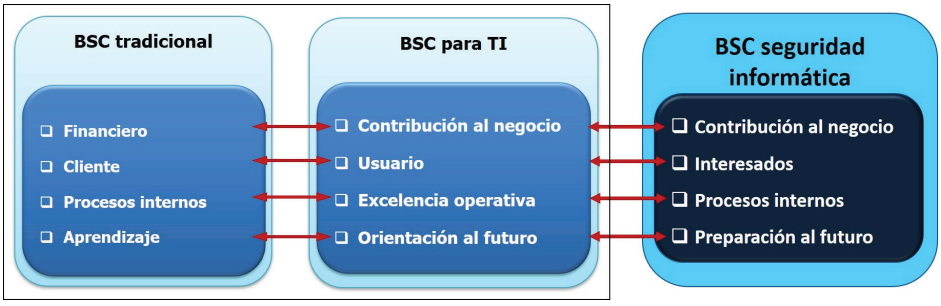

Figura 5. Correspondencia entre el BSC tradicional, BSC para TI y el BSC para seguridad informática

Elaboración propia

El componente de contribución al negocio tiene como función agregar valor al mismo negocio y valor a la función de seguridad de TI. Los interesados deben recibir los servicios de seguridad adecuados en función de sus roles y responsabilidades.

Los procesos internos están orientados a entregar productos y servicios de seguridad considerando aspectos de costos, eficiencia y recursos. Y finalmente, el componente de preparación al futuro implica un proceso de mejora continua en seguridad informática que permita hacer frente a los desafíos (vulnerabilidades, tipos de ataques, etc.) del futuro.

3.2 CONTROLES CIS

Los 20 controles críticos de CIS abordan los aspectos básicos, técnicos y de gestión de la seguridad informática y pueden tener una analogía con otros *frameworks* o estándares como ISO/IEC 27002 y NIST 800-53.

Para el estudio es necesario establecer qué controles se pueden automatizar para que sirvan como entrada para el tablero de mando integral de seguridad informática. Como referencia inicial se considera que pueden automatizar ciertos controles de NIST 800.53 (Montesino *et al.*, 2012), tal como se muestra en la figura 2. Si se toma esta información, se puede realizar un *benchmark* con los controles de CIS y determinar qué controles específicos pueden automatizarse.

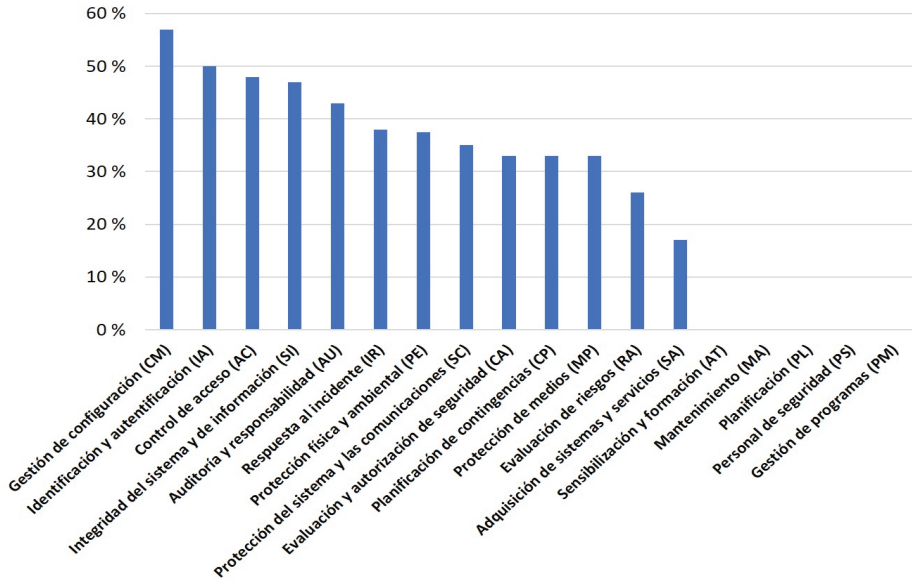

Figura 6. Porcentaje de controles automatizables en las diferentes familias de NIST SP 800-53

Fuente: Montesino, Fenz y Baluja, 2012

Tomando como referencia la figura 6 y el análisis comparativo se determinan los controles que son susceptibles de ser automatizados en la información de entrada, es decir, que para efectos de la alimentación de datos en el tablero de mando integral por cada indicador se puede hacer uso de herramientas cuyos reportes o datos pueden ser transferidos de forma automática. Los controles CIS que pueden ser automatizados se muestran en la tabla 1. Cabe recalcar que para el proceso de automatización se pueden considerar las herramientas mencionadas en la descripción de los controles de seguridad. Para la aplicación en cada caso se debe elaborar la declaración de aplicabilidad considerando la pertinencia y capacidades organizacionales.

Tabla 1
Controles de CIS que pueden ser automatizados

Control	Subcontrol	
[01] Inventario y control de activos de *hardware*	01.1	Utilizar una herramienta de descubrimiento activo
	01.2	Utilizar una herramienta de descubrimiento pasivo de activos
	01.3	Utilizar DHCP Logging para actualizar el inventario de activos
	01.4	Mantener un inventario de activos detallado
	01.5	Mantener la información del inventario de activos

(*continúa*)

(*continuación*)

Control	Subcontrol
[02] Inventario y control de activos *software*	02.1 Mantener un inventario de *software* autorizado 02.3 Utilizar herramientas de inventario de *software* 02.4 Rastrear información del inventario de *software* 02.5 Integrar los inventarios de activos de *hardware* y *software* 02.7 Utilizar lista blanca de aplicaciones
[03] Gestión continua de vulnerabilidades	03.1 Ejecutar herramientas de escaneo automatizados de vulnerabilidades
[04] Uso controlado de privilegios administrativos	04.1 Mantener un inventario de cuentas administrativas 04.4 Usar contraseñas únicas
[05] Configuración segura para *hardware* y *software* en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	05.2 Mantener imágenes seguras
[07] Protección de correo electrónico y navegador web	07.1 Asegurar el uso de navegadores y clientes de correo electrónico que cuenten con soporte
[08] Defensa contra *malware*	08.1 Utilizar *software antimalware* de gestión centralizada 08.2 Asegurar que el *software antimalware* y las firmas estén actualizadas
[12] Defensa de borde	12.11 Requerir autenticación multifactor en todos los inicios de sesión remotos 12.12 Gestionar todos los dispositivos remotos que se conectan a la red interna
[13] Protección de datos	13.1 Mantener un inventario de información sensible 13.3 Monitorear y bloquear el tráfico de red no autorizado 13.5 Monitorear y detectar cualquier uso no autorizado de cifrado
[14] Control de acceso basado en la necesidad de conocer protección de datos	14.5 Utilizar una herramienta de descubrimiento activo para identificar datos sensibles
[15] Control de acceso inalámbrico	15.1 Mantener un inventario de puntos de acceso inalámbrico autorizados 15.2 Detectar puntos de acceso inalámbricos conectados a la red cableada
[16] Monitoreo y control de cuentas	16.1 Mantener un inventario de sistemas de autenticación 16.2 Configurar un punto de autenticación centralizado 16.3 Requerir autenticación multifactor 16.6 Mantener un inventario de cuentas 16.12 Monitorear los intentos de acceso a cuentas desactivadas 16.13 Alertar sobre desviación de comportamiento de inicio de sesión de cuentas
[18] Seguridad del *software* de aplicación	18.3 Verificar que el *software* adquirido aún tiene soporte 18.9 Sistemas separados de producción y no producción

Elaboración propia

4. RESULTADOS

Para la formulación del modelo de evaluación de controles se realizó la alineación del Balanced Scorecard (BSC) con los controles de CIS, quedando distribuido tal como se muestra en la figura 7. Los 20 controles CIS han sido distribuidos en cada cuadrante del Balanced Scorecard predominando en procesos internos la mayor cantidad de controles (ocho en total), mientras que en el otro extremo el cuadrante Preparación para el futuro solo incluye el control 17 de CIS ("Implementar un programa de concienciación y entrenamiento de seguridad"); del mismo modo, los cuadrantes Interesados y Contribución al negocio tienen 5 y 6 controles CIS respectivamente.

Figura 7. Modelo de BSC con los controles CIS

Elaboración propia

Cada control CIS está compuesto por subcontroles que determinan los indicadores a monitorizar y medir. Estos indicadores poseen unidades propuestas por el modelo, pero cuyos valores deben ser ajustados a cada caso donde se aplique el modelo.

Los controles CIS se agrupan en tres dominios: básicos, fundamentales y organizacionales, que en la tabla 2 se observa en un grado de correspondencia entre los controles de cada grupo o dominio de CIS con los controles considerados en los cuadrantes del tablero de mando. De esta forma, se evidencia que los considerados en el cuadrante Procesos internos corresponde a la mayoría de los controles básicos y algunos del grupo de fundamentales de CIS; del mismo modo, los controles considerados en el cuadrante de Interesados corresponden en su mayoría a los controles fundamentales de CIS; y finalmente los controles de los cuadrantes Contribución al negocio y Preparación para el futuro corresponden mayoritariamente a los controles organizacionales de CIS. Esto supone una alineación lógica entre el tablero de mando integral y los dominios de CIS.

Tabla 2
Correspondencia entre los controles CIS y los cuadrantes del BSC

Cuadrantes de BSC	Dominios de controles CIS
Procesos internos 01.0 Inventario y control de activos de *hardware* 02.0 Inventario y control de activos *software* 05.0 Configuración segura para *hardware* y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores 06.0 Mantenimiento, monitoreo y análisis de logs de auditoría 08.0 Defensa contra *malware* 09.0 Limitación y control de puertos de red, protocolos y servicios 10.0 Capacidad de recuperación de datos 11.0 Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores.	**Básicos** 01.0 Inventario y control de activos de *hardware* 02.0 Inventario y control de activos *software* 03.0 Gestión continua de vulnerabilidades 04.0 Uso controlado de privilegios administrativos 05.0 Configuración segura para *hardware* y *software* en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores 06.0 Mantenimiento, monitoreo y análisis de *logs* de auditoría
Interesados 04.0 Uso controlado de privilegios administrativos 07.0 Protección de correo electrónico y navegador web 12.0 Defensa de borde 15.0 Control de acceso inalámbrico 16.0 Monitoreo y control de cuentas	**Fundamentales** 07.0 Protección de correo electrónico y navegador web 08.0 Defensa contra *malware* 09.0 Limitación y control de puertos de red, protocolos y servicios 10.0 Capacidad de recuperación de datos 11.0 Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores 12.0 Defensa de borde 13.0 Protección de datos 14.0 Control de acceso basado en la necesidad de conocer protección de datos 15.0 Control de acceso inalámbrico
Contribución al negocio 03.0 Gestión continua de vulnerabilidades 13.0 Protección de datos 14.0 Control de acceso basado en la necesidad de conocer protección de datos 18.0 Seguridad del *software* de aplicación 19.0 Respuesta y manejo de incidentes 20.0 Pruebas de penetración y ejercicios de *red team*	**Organizacional** 16.0 Monitoreo y control de cuentas 17.0 Implementar un programa de concienciación y entrenamiento de seguridad 18.0 Seguridad del *software* de aplicación 19.0 Respuesta y manejo de incidentes 20.0 Pruebas de penetración y ejercicios de *red team*
Preparación para el futuro 17.0 Implementar un programa de concienciación y entrenamiento de seguridad.	

Elaboración propia

Se generó una primera versión del tablero de mando integral cuya aplicación se realizó en cinco instituciones educativas durante el año 2019 (ver figura 8) y por medio de una encuesta de satisfacción de pudo comprobar el grado de efectividad en la evaluación de los controles de seguridad informática que corresponden a este caso, además de facilitar la visualización del estado de los mecanismos de seguridad implementados y tomar las decisiones necesarias para reforzar o corregir los niveles de seguridad en la organización.

Balanced Scorecard - Tablero de mando integral de seguridad informática

Institución: **Año:** 2019

Cuadrantes	Control CIS	Nombre del control	Esperado	Estado actual	Detalle
Procesos internos	01	Inventario y control de activos de *hardware*	1	0,49	Detalle CIS01
	02	Inventario y control de activos *software*	1	0,35	Detalle CIS02
	05	Configuración segura para *hardware* y *software* en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	1	0,00	Detalle CIS05
	06	Mantenimiento, monitoreo y análisis de logs de auditoria	1	0,00	Detalle CIS06
	08	Defensa contra *malware*	1	0,00	Detalle CIS08
	09	Limitación y control de puertos de red, protocolos y servicios	1	0,00	Detalle CIS09
	10	Capacidad de recuperación de datos	1	0,00	Detalle CIS10
	11	Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores	1	0,00	Detalle CIS11
Interesados	04	Uso controlado de privilegios administrativos	1	0,00	Detalle CIS04
	07	Protección de correo electrónico y navegador web	1	0,00	Detalle CIS07
	12	Defensa de borde	1	0,00	Detalle CIS12
	15	Control de acceso inalámbrico	1	0,00	Detalle CIS15
	16	Monitoreo y control de cuentas	1	0,00	Detalle CIS16
	03	Gestión continua de vulnerabilidades	1	0,00	Detalle CIS03

Figura 8. Aplicativo del Modelo de BSC con los controles CIS

Elaboración propia

En la tabla 3 se muestran los resultados de la encuesta de satisfacción de cinco instituciones de educación como casos de estudio, y de acuerdo con estos resultados se evidencia que la herramienta tiene que mejorar la calidad de las interfaces gráficas (presentación visual) y la facilidad de manejo. Sin embargo, la contribución hacia la representación de los controles CIS para el monitoreo y seguimiento de los indicadores resulta positivo, sumando a ello que, según lo aplicado, sí refleja los controles que deben ser medidos en la organización.

Tabla 3
Encuesta de satisfacción sobre el uso de la herramienta

Enunciado	Totalmente de acuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en desacuerdo
El tablero es fácil de manejar.			4 (80 %)	1 (20 %)	
Los cuadrantes del tablero de mando integral reflejan los procesos de seguridad de la organización.		3 (60%)	2 (40 %)		
El tablero de mando integral de seguridad ayuda a realizar el seguimiento del estado de los controles de seguridad de la organización.		4 (80 %)	1 (20 %)		
Se pueden adaptar los controles a la realidad específica de la organización.		4 (80 %)	1 (20 %)		

Elaboración propia

A diferencia de los modelos de BSC relacionados con la seguridad de la información, la propuesta presentada es un esfuerzo por integrar y articular los datos y mediciones desde los niveles operativos como insumos directos para la herramienta del sistema de gestión estratégica en términos de seguridad alineado a los objetivos institucionales del negocio.

La propuesta formulada en esta investigación trata de mantener una representación del Cuadro de Mando Integral en su forma esencial; no obstante, se pretende que el enfoque sea más amplio, involucrando no solo los controles definidos por el CIS, sino también nuevos controles orientados a la identificación, comprensión y proyección de las necesidades de los usuarios y organizaciones, en línea con el modelo de ciberconciencia situacional (Gutzwiller, Hunt y Lange, 2016). Asimismo, un modelo integrado de controles en seguridad puede incorporar técnicas de OSINT (inteligencia de fuentes abiertas) para el reconocimiento de la información organizacional expuesta relacionada con los controles de gestión de incidentes de seguridad que puedan derivar en mecanismos automatizados de notificación a los equipos de respuesta ante incidentes de seguridad (CSIRT, por sus siglas en inglés) haciendo uso del vocabulario para el registro de eventos y el intercambio de incidentes (VERIS, por sus siglas en inglés). Se prevé, asimismo, que los programas de entrenamiento y concienciación se articulen alrededor de la retroalimentación obtenida por una adecuada medición de los controles y tengan un efecto positivo en el proceso de gestión de seguridad de la información.

5. CONCLUSIONES

Los controles definidos por el CIS (Center of Internet Security) son susceptibles de ser categorizados en alguno de los cuadrantes del tablero de mando integral (Balanced Scorecard) y en general la mayoría de los controles básicos CIS se alinean con el cuadrante de Procesos internos del BSC, los controles de Fundamentales CIS se alinean con el cuadrante de Interesados del BSC y los controles Organizacionales CIS se alinean con el cuadrante de Contribución al negocio y Preparación para el futuro.

El desafío de disponer de los datos oportunamente requiere de un ordenamiento en los procedimientos para obtener, transmitir y almacenarlos. En general, los datos tienen que ser obtenidos de forma manual, por lo que puede conllevar a márgenes de error y oportunidad. Asimismo, se ha identificado qué tipo de datos se pueden automatizar en su proceso de recolección y alimentación para el tablero de mando integral de seguridad. Entre los controles que pueden automatizarse se mencionan los siguientes: inventario de activos (*hardware* y *software*), gestión de cuentas, gestión de *logs*, monitoreo de sistemas, protección contra *malware*, Gestión de actualizaciones y escaneo de vulnerabilidades, *backup* de información, y gestión de incidentes.

El modelo de Balanced Scorecard para el monitoreo de los 20 controles críticos de seguridad informática del CIS (Center for Internet Security) es un acercamiento inicial para ofrecer a las organizaciones una herramienta efectiva para el seguimiento y control de indicadores de seguridad. Para facilitar la aplicación del modelo se ha construido un aplicativo con macros junto al proceso de ingreso de datos y actualización sencilla. En vista de los resultados obtenidos, se ha validado favorablemente la aplicación de BSC y se han identificado diversas oportunidades para beneficiarse de un cuadro de control unificado en la gestión de la seguridad de la información.

6. TRABAJOS FUTUROS

Un aspecto importante que queda pendiente en la investigación es realizar pruebas con alimentación de datos de forma automatizada haciendo uso de herramientas existentes como los SIEM mencionados en este trabajo, de tal forma que los controles que son susceptibles de implementarse basados en estas entradas sean evaluados en términos de efectividad.

Asimismo, se debe extender el análisis respecto al alcance del modelo para cubrir aspectos de ciberconciencia situacional, inteligencia de amenazas y los procesos de intercambio de información con organismos públicos o equipos de respuesta a incidentes de seguridad. También, analizar la inclusión en el modelo para la medición de exposición de datos sensibles y confidenciales las técnicas de OSINT (inteligencia de fuentes abiertas).

Es preciso, también, desarrollar la herramienta basada en una plataforma estandarizada para el intercambio de datos (tecnologías web, bases de datos, entre otras) de tal forma que las consultas y reportes históricos sean accesibles y organizados de forma más eficiente.

REFERENCIAS

AT&T Cybersecurity. (2020). AlienVault OSSIM. Recuperado de https://cybersecurity.att.com/products/ossim

Caudle, S. (2008). The Balanced Scorecard: A Strategic Tool in Implementing Homeland Security Strategies. *Homeland Security Affairs*, *4*(3).

CIS (Center for Internet Security). (2018). Homepage. Recuperado de https://www.cisecurity.org/

CNSS. (2015). Committee on National Security Systems (CNSS) Glossary. *CNSS Instruction*. https://doi.org/10.1016/0020-7292(88)90192-0

DeLooze, L. L. (2006). Creating a Balanced Scorecard for Computer Security. *2006 IEEE Information Assurance Workshop*, 15-18. https://doi.org/10.1109/IAW.2006.1652071

Grembergen, W. Van. (2005). *Strategies for information technology governance*. (J. Travers, M. Khosrow-Pour y A. Appicello, Eds.). Londres: Idea Group Inc. https://doi.org/10.4018/978-1-59140-140-7

Groš, S. (2019). A Critical View on CIS Controls. *Cornell University*. Recuperado de http://arxiv.org/abs/1910.01721

Gutzwiller, R. S., Hunt, S. M. y Lange, D. S. (2016). A Task Analysis toward Characterizing Cyber-Cognitive Situation Awareness (CCSA) in Cyber Defense Analysts. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, CogSIMA 2016*, (Marzo), 14-20. https://doi.org/10.1109/COGSIMA.2016.7497780

Herath, T., Herath, H. y Bremser, W. G. (2010). Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management. *Information Systems Management*, *27*(1), 72-81. https://doi.org/10.1080/10580530903455247

IBM. (2020). Security information and event management (SIEM). Recuperado de https://www.ibm.com/security/security-intelligence

Indecopi. (2014). *Norma Técnica Peruana NTP-ISO/IEC 27001-2014. Tecnología de la Información*. Lima: Indecopi.

Industria de tarjetas de pago (PCI). Norma de seguridad de datos. Requisitos y procedimientos de evaluación de seguridad. Versión 3.2. (2016). *PCI Securiry Standards Council*. Recuperado de https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3-2_es-LA.pdf

ISO/IEC. (2013). International Standard ISO/IEC-27002-2013. Switzerland.

Johnson, L. (2015). *Security Controls Evaluation, Testing, and Assessment Handbook*. (C. Katsaropoulos, Ed.), Security Controls Evaluation, Testing, and Assessment Handbook. Walthman: Elsevier. https://doi.org/10.1016/C2013-0-13416-2

Kaplan, R. y Norton, D. (2002). *Cuadro de Mando Integral* (The Balanced Scorecard). Barcelona: Ediciones Gestion 2000.

Kaplan, R. S. y Norton, D. P. (1996). The Balanced Scorecard: Translating Strategy Into Action. Proceedings of the IEEE. https://doi.org/10.1109/JPROC.1997.628729

Kaplan, R. S. y Norton, D. P. (2005). *Cómo utilizar el Cuadro de Mando Integral*. Barcelona: Gestión 2000.

Keyes, J. (2005). *Implementing the IT Balanced Scorecard. Auerbach Publications (first)*. Florida: Auerbach Publications. Recuperado de http://doi.wiley.com/10.1002/jcaf.20198

Marchand-Niño, W. R. (2013). Metodología de implantación del modelo Balanced Scorecard para la gestión estratégica de TIC. Caso: Universidad Nacional Agraria de la Selva. *PIRHUA-Universidad de Piura*. Recuperado de https://hdl.handle.net/11042/1842

Martinsons, M., Davison, R. y Tse, D. (1999). The Balanced Scorecard: a Foundation for the Strategic Management of Information Systems. *Decision Support Systems*, *25*(1), 71-88. https://doi.org/10.1016/S0167-9236(98)00086-4

Montesino, R., Fenz, S. y Baluja, W. (2012). SIEM-based framework for security controls automation. *Information Management & Computer Security*, *20*(4), 248-263. https://doi.org/10.1108/09685221211267639

NIST Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations. Sp-800-53Ar4, 462. (2014). *National Institute of Standards and Technology* https://doi.org/10.6028/NIST.SP.800-53Ar4

Perminov, P., Kosachenko, T., Konev, A., & Shelupanov, A. (2020). Automation of Information Security Audit in the Information System on the Example of a Standard "cis Palo Alto 8 Firewall Benchmark." *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(2), 2085–2088. https://doi.org/10.30534/ijatcse/2020/182922020

Splunk® Enterprise Security (2020). *Splunk*. Recuperado de https://www.splunk.com/en_us/software/enterprise-security.html