



COLECCIÓN

ASÍ HABLA  
EL EXTERNADO

4

# DISRUPCIÓN TECNOLÓGICA, TRANSFORMACIÓN DIGITAL Y SOCIEDAD



AIRES DE REVOLUCIÓN:  
NUEVOS DESAFÍOS TECNOLÓGICOS A LAS  
INSTITUCIONES ECONÓMICAS, FINANCIERAS Y  
ORGANIZACIONALES DE NUESTROS TIEMPOS

Editores:

Juan Carlos Henao  
Liliana López-Jiménez

Coordinadora general de la obra:

Constanza García Chaves

Universidad  
**Externado**  
de Colombia

135  
Años

JUAN CARLOS  
HENA O  
LILIANA  
LÓPEZ-JIMÉNEZ  
Editores

DISRUPCIÓN TECNOLÓGICA,  
TRANSFORMACIÓN DIGITAL  
Y SOCIEDAD

TOMO IV  
AIRES DE REVOLUCIÓN: NUEVOS DESAFÍOS  
TECNOLÓGICOS A LAS INSTITUCIONES ECONÓMICAS,  
FINANCIERAS Y ORGANIZACIONALES  
DE NUESTROS TIEMPOS

UNIVERSIDAD EXTERNADO DE COLOMBIA

*Disrupción tecnológica, transformación digital y sociedad. Tomo IV, Aires de revolución : nuevos desafíos tecnológicos a las instituciones económicas, financieras y organizacionales de nuestros tiempos / Jhon Alirio Sanabria Téllez [y otros] ; Juan Carlos Henao, Liliana López-Jiménez (eds.). — Bogotá : Universidad Externado de Colombia. 2021.*

493 páginas : gráficos ; 24 cm. (Así habla el externado)

Incluye referencias bibliográficas.

ISBN: 9789587905861

1. Tecnologías disruptivas 2. Economía -- Innovaciones tecnológicas 3. Innovaciones tecnológicas -- Aspectos sociales 4. Cambio tecnológico -- Aspectos sociales 5. Empleo -- Innovaciones tecnológicas I. Henao Pérez, Juan Carlos, 1958- , editor II. Universidad Externado de Colombia III. Título IV. Serie

303.4833 SCDD 21

Catalogación en la fuente -- Universidad Externado de Colombia. Biblioteca. EAP.

abril de 2021

ISBN 978-958-790-586-1

© 2021, JUAN CARLOS HENAO Y LILIANA LÓPEZ-JIMÉNEZ (EDITORES)

© 2021, UNIVERSIDAD EXTERNADO DE COLOMBIA

Calle 12 n.º 1-17 este, Bogotá

Teléfono (57 1) 342 0288

publicaciones@uexternado.edu.co

www.uexternado.edu.co

Primera edición: abril de 2021

Diseño de cubierta: Departamento de Publicaciones

Corrección de estilo: Óscar Torres Angarita

Composición: María Libia Rubiano

Impresión y encuadernación: Xpress Estudio Gráfico y Digital S.A.S. - Xpress Kimpres

Tiraje: de 1 a 1.000 ejemplares

Impreso en Colombia

*Printed in Colombia*

Prohibida la reproducción o cita impresa o electrónica total o parcial de esta obra, sin autorización expresa y por escrito del Departamento de Publicaciones de la Universidad Externado de Colombia. Las opiniones expresadas en esta obra son responsabilidad de los autores.

LILIANA LÓPEZ-JIMÉNEZ\*  
JORGE BEJARANO-LOBO\*\*

*¿Es efectiva la gestión en seguridad digital de los bancos  
de América Latina y el Caribe?\*\*\**

*Infosec management among banks in Latin America  
and the Caribbean: Is it effective?*

## RESUMEN

Este estudio usa datos recogidos por la Organización de Estados Americanos (OEA) en un cuestionario aplicado a 191 bancos de América Latina y el Caribe en 2018, para explorar qué tan efectivas son las prácticas de gestión de seguridad de la información (Seginfo) de los bancos de la región para detectar internamente eventos adversos. El estudio identificó que la adopción de marcos y estándares de Seginfo y la implementación de medidas técnicas, procesos y sistemas para Seginfo contribuyen a la efectividad de la gestión. Al contrario, el apoyo de la alta gerencia y algunos esfuerzos por robustecer y entrenar personal en Seginfo no están asociados con una mayor efectividad.

## PALABRAS CLAVE

Ciberseguridad, seguridad de la información (Seginfo), estándares Seginfo, detección interna de ataques, impacto económico.

## INFOSEC MANAGEMENT AMONG BANKS IN LATIN AMERICA AND THE CARIBBEAN: IS IT EFFECTIVE?

## ABSTRACT

Our study uses data gathered by the Organization of American States (OAS) in a survey applied to 191 banks in Latin America and the Caribbean in 2018, and then analyze these data to explore how effective some information security (Infosec) management practices carried out by banks in the region are in increasing internal breach detection capabilities. Our findings

---

\* PhD Business Administration. Profesora de la Facultad de Administración de Empresas, Universidad Externado de Colombia. Correo-e: liliana.lopez@uexternado.edu.co

\*\* Candidato a doctor en Ingeniería Informática. Profesor de posgrado de la Facultad de Administración de Empresas y del Departamento de Derecho Informático, Universidad Externado de Colombia. Correo-e: jfbejarano@techandlaw.com.co

\*\*\* Los autores agradecen a Belisario Contreras, gerente del Programa de Ciberseguridad de la Organización de Estados Americanos, por su apoyo en la realización del estudio; a Estefanía Fernández, administradora de empresas de la Universidad Externado de Colombia, por su asistencia en el proceso de investigación, y a dos evaluadores anónimos por sus comentarios.

suggest that the adoption of Infosec standards and frameworks, and the implementation of technical measures, processes and IT for Infosec are related to higher effectiveness. Conversely, we found that top management support and some reported efforts to strengthen and train the workforce in Infosec are not associated with increased effectiveness.

Keywords: cybersecurity, information security (Infosec), Infosec standards, security breaches, economic impact.

## INTRODUCCIÓN

Un pilar de la economía digital es la seguridad de las transacciones financieras realizadas a través de internet. Según investigaciones de mercados realizadas por *Business Insider Intelligence*, para 2018 el 89 % de los consumidores de servicios financieros en Estados Unidos usaban servicios de banca móvil, y los porcentajes eran aún mayores para las personas más jóvenes en la fuerza laboral. Para estos mismos consumidores, la calidad de la experiencia en línea es un factor clave a la hora de seleccionar un banco para manejar sus operaciones, y esta experiencia incluye aspectos de funcionalidad relacionados con la seguridad de las transacciones (Meola, 2019).

En América Latina, un estudio reciente hecho a bancos de la región encontró que, para 79 % de los bancos encuestados, internet es ya uno de los tres canales más usados, y que la seguridad de las transacciones es una de las principales preocupaciones manifestadas por los usuarios que no han adoptado ninguna modalidad de banca digital (Technisys, 2016).

Entendiendo la importancia de la seguridad de la información (Seginfo) en el contexto de la creciente digitalización de los servicios bancarios, la Organización de Estados Americanos (OEA) comisionó a un equipo de expertos para elaborar un estudio sobre este tema. El estudio, titulado “Ciberseguridad: estado del sector bancario en América Latina y el Caribe” y publicado en 2018, establece una caracterización del estado de la Seginfo en los bancos de los países de América Latina y el Caribe (OEA, 2018), y es un punto de partida invaluable para conocer el nivel de preparación y las capacidades de respuesta y de recuperación, tanto en lo tecnológico como en lo administrativo, de los bancos de la región frente a amenazas y a ataques que atenten contra la seguridad de su información digital.

El estudio recogió datos directamente de 191 bancos de la región mediante un formulario de encuesta diseñado por los autores, y los analizó con

instrumentos de analítica descriptiva, diferenciando los resultados por varios criterios, particularmente por tamaño del banco. Por tal razón, el informe permite saber, por ejemplo, si los bancos grandes están mejor preparados que los pequeños, o si los pequeños han sufrido más ataques que los grandes.

Adicionalmente, los datos capturados en dicha encuesta podrían analizarse a la luz de métodos de estadística inferencial, y particularmente con modelos econométricos estructurales que permitan determinar si existen correlaciones entre los diferentes temas explorados en el estudio. Por ejemplo, dado que el estudio captura datos tanto sobre las prácticas de gestión en Seginfo como sobre el impacto de los ataques, es posible entonces preguntarse si el uso de estas prácticas está asociado con beneficios tales como la detección interna de ataques o la reducción en los costos de respuesta y recuperación de dichos ataques.

El presente trabajo busca entonces usar la base de datos del ya mencionado estudio de la OEA para abordar tales análisis, orientados por una pregunta guía: ¿qué tan efectivas han resultado prácticas, formales e informales, tales como el apoyo de la alta gerencia, la adopción de estándares de gestión de Seginfo y la capacitación a empleados en Seginfo, en ayudar a los bancos de la región a obtener mejores resultados en su gestión de Seginfo?

El capítulo está organizado en seis secciones, así: terminada esta primera sección introductoria, la segunda sección ampliará la presentación del estudio publicado por la OEA, del cual se obtienen los datos para el presente trabajo. La tercera sección recoge las principales discusiones y hallazgos de la literatura académica internacional en Seginfo, con respecto a los temas abordados en el estudio de la OEA, y con base en ello plantea algunas hipótesis. La cuarta sección presenta el diseño metodológico empleado para extraer y analizar los datos tomados del estudio de la OEA. En particular, explica cuáles datos en específico se tomaron de dicho estudio, y cómo se trataron para poder crear un modelo econométrico que permitiera corroborar las hipótesis planteadas. La quinta sección muestra los hallazgos de este trabajo, incluyendo la corroboración de las hipótesis planteadas. La sexta y última sección contrasta la discusión de la literatura académica revisada en la sección 3 frente a los hallazgos del presente trabajo y, a manera de conclusión, ofrece como nuevo aporte unas recomendaciones e implicaciones para la práctica del sector bancario y la futura investigación académica.

## I. EL ESTUDIO DE LA OEA

Los autores del estudio de la OEA usaron dos fuentes de datos para realizar la caracterización: una encuesta realizada a funcionarios de los bancos de la región, la cual recoge datos de 191 entidades bancarias ubicadas en 19 países, y una segunda encuesta realizada a 722 usuarios de los servicios de estos mismos bancos.

El trabajo reportado en el presente capítulo se concentra en la primera de estas fuentes, y por consiguiente solo esta fuente será descrita a continuación.

El instrumento de encuesta se organizó en tres secciones: la primera con preguntas de caracterización de la entidad bancaria, la segunda con preguntas sobre las prácticas de gestión de Seginfo y la ocurrencia de eventos e incidentes de Seginfo, y la tercera con preguntas relacionadas con el impacto de los incidentes sobre los resultados financieros de la entidad. Los datos se recogieron de manera confidencial y anónima, y se trabajaron de manera agregada (OEA, 2018).

En el bloque de *preguntas de caracterización* se destacan ítems sobre el tamaño de la entidad y su presupuesto de Seginfo. En el segundo bloque, las *preguntas de gestión de Seginfo* abordan específicamente temas sobre modelo de gobierno de Seginfo (p. ej., jerarquía en la toma de decisiones y apoyo de la alta gerencia), preparación organizacional para Seginfo (p. ej., adopción de estándares internacionales en Seginfo, uso de herramientas, controles o procesos de Seginfo), capacitación y concientización a empleados, mientras que las *preguntas sobre eventos* (ataques exitosos y no exitosos) e incidentes (ataques exitosos) exploran la frecuencia y tipología de estos ataques, así como los mecanismos de reporte. Finalmente, el tercer bloque, correspondiente a las *preguntas de impacto*, explora los costos de respuesta y recuperación de incidentes, y el retorno sobre la inversión en Seginfo.

En resumen, el estudio de la OEA recoge datos sobre una gran variedad de aspectos relacionados con la gobernanza y la gestión de la Seginfo en los bancos latinoamericanos y del Caribe, los cuales pueden ayudar a explicar el desempeño de estos mismos bancos frente a la ocurrencia de ataques y al impacto económico de dichos ataques para estas entidades.

## 2. REVISIÓN DE LITERATURA

Resulta claro que los datos recogidos para el estudio de la OEA pueden usarse para identificar posibles asociaciones entre variables relacionadas con la

gobernanza y la gestión de la Seginfo, por un lado, y variables relacionadas con el desempeño de los bancos en cuanto a Seginfo, medido por medio de la ocurrencia de ataques y de su impacto económico.

Por esta razón, se consideró importante explorar la literatura académica internacional frente a los temas mencionados, organizados en cinco bloques: gobernanza y apoyo de la alta gerencia, prácticas de gestión, aspectos de gestión de empleados, ocurrencia y detección de ataques, y consecuencias económicas.

Para identificar literatura pertinente se realizaron búsquedas en EBS-coHost y Google académico. Se usó el término “information security” combinado con términos en inglés relacionados con cada uno de los temas identificados en el estudio de la OEA, junto con sus respectivos subtemas. Por ejemplo, se realizaron búsquedas así: “INFORMATION SECURITY” y “top management support”, “information security” y “standards”, o “information security” y “economic / financial impact”, entre otras.

En Google Scholar se seleccionaron artículos de revista publicados a partir del año 2000 y que aparecieran en las dos primeras páginas de resultados del buscador. Dado que Google académico organiza los resultados con base en el número de citas de cada entrada, concentrarse en los resultados de las dos primeras páginas asegura que se retienen los resultados que han tenido más influencia en la conversación académica sobre el tema. Un riesgo de este criterio de selección consiste en descartar artículos publicados recientemente, que pese a ser relevantes pueden no haber alcanzado aún un amplio número de citas. Por esta razón, los resultados anteriores se complementaron con una búsqueda idéntica en el motor de Ebsco Host, que recogiera artículos publicados a partir del año 2015.

Los artículos resultantes se filtraron para retener solo aquellos cuyo contenido realmente trataba a profundidad uno o varios de los cinco temas mencionados.

Esta sección describe la comprensión alcanzada por los autores con respecto a la literatura académica internacional en el tema de Seginfo en las organizaciones. Esta revisión de literatura está organizada alrededor de cuatro de los cinco temas<sup>1</sup> que explora el estudio de la OEA acerca de la gestión de los bancos, a saber: i) modelo de gobierno y apoyo de la alta gerencia a Seginfo,

---

1 Los artículos encontrados que tratan el tema “ocurrencia y detección de ataques” lo hacen generalmente a la luz del impacto económico de dichos ataques o de las prácticas de gestión que

ii) buenas prácticas en gestión de TI / Seginfo, iii) aspectos relacionados con la gestión de personal frente a Seginfo y iv) impacto de los ataques.

## 2. I MODELO DE GOBIERNO Y APOYO DE LA ALTA GERENCIA

La gobernanza de Seginfo consiste en el liderazgo, las estructuras organizacionales y los procesos que salvaguardan los activos críticos de información en una organización (Nicho, 2018). Se encontraron muy pocos estudios empíricos que atiendan los temas de gobernanza abarcados por el estudio de la OEA, tales como los niveles jerárquicos entre el CEO y la máxima autoridad de Seginfo, o el reporte periódico a la junta directiva acerca de la gestión de Seginfo.

Los estudios consultados han encontrado que el rol llamado *chief information security officer* está creciendo en popularidad (Karanja & Rosso, 2017), y que tanto la contratación de personas en este rol y la formalización de estructuras para el gobierno de Seginfo han surgido de manera reactiva, como respuesta de las organizaciones a ciberataques de los cuales han sido víctimas (Karanja, 2017). Más relevante a nuestro trabajo, un estudio identificó que las firmas en donde la máxima autoridad de Seginfo se encuentra en un nivel más alto en la jerarquía se recuperan más rápidamente de los efectos financieros negativos causados por ciberataques (Zafar *et al.*, 2016), con lo cual se puede esperar de manera más general que el fortalecimiento de la gobernanza en Seginfo tenga un impacto positivo en los resultados financieros de los bancos (Zafar *et al.*, 2016).

Por su parte, el apoyo de la alta gerencia ha sido estudiado con amplitud en la literatura, típicamente como un factor determinante de una gestión adecuada en Seginfo. En principio, se ha visto que el apoyo de la alta gerencia contribuye a una gestión más proactiva en la prevención de ataques (Kankanhalli *et al.*, 2003), a una mejor actitud y cumplimiento de las políticas de Seginfo por parte de los empleados (Cuganesan *et al.*, 2018; Hu *et al.*; 2012; Ifinedo 2016; Kankanhalli *et al.*, 2003; Knapp *et al.*, 2006), a una cultura más sensible a la importancia de la seguridad de la información (Knapp *et al.*, 2006), y en general a un mejor desempeño en la gestión de

---

pueden minimizar los riesgos de Seginfo, y por lo tanto fueron reubicados en alguno de estos bloques según correspondiera.

Seginfo (Soomro *et al.*, 2016; Tu *et al.*, 2018) y a una menor ocurrencia de ataques informáticos (Kwon *et al.*, 2013).

Algunos estudios han buscado identificar los mecanismos puntuales a través de los cuales la alta gerencia afecta el desempeño en Seginfo. De manera general, se ha concluido que la alta gerencia aporta al desempeño en Seginfo a través de la formulación y ejecución de una política de Seginfo (Bauer & Bernroider, 2017), de la creación de normas de comportamiento favorables a Seginfo (Cuganesan *et al.*, 2018), del desarrollo de actividades de concientización y capacitación para los empleados (Bauer & Bernroider, 2017; Tu *et al.*, 2018), de la generación de un ambiente en donde los empleados desarrollen más confianza en sus capacidades de cumplir con las políticas de Seginfo (Humaidi & Balakrishnan, 2018), y de la facilitación para la implementación de herramientas, procesos y controles de Seginfo (Tu *et al.*, 2018).

Si bien el estudio de la OEA no usa instrumentos validados en la academia para capturar información sobre el apoyo de la alta gerencia, es destacable que las preguntas realizadas en este informe coinciden con la operacionalización empírica más extendida de este constructo en la literatura, la cual consiste en indagar sobre comportamientos que evidencien apoyo e interés, tales como la asistencia a reuniones sobre Seginfo, el involucramiento en decisiones relacionadas con Seginfo, y el monitoreo de actividades en Seginfo (Gordon & Loeb, 2006; Humaidi & Balakrishnan, 2018; Ifinedo, 2016; Kankanhalli *et al.*, 2003; Knapp *et al.*, 2006).

Lamentablemente, como reportan Cuganesan y sus colegas (2018), no toda la literatura sobre este tema es concluyente respecto a los efectos positivos del apoyo de la alta gerencia sobre el desempeño en Seginfo.

Por todo lo anterior, los autores de este trabajo consideran pertinente formular un constructo titulado *gobernanza y apoyo de la alta gerencia*, que recoja los ítems del cuestionario de la OEA relacionados en estos temas, para ser usado en el modelo teórico a corroborar empíricamente, y formular la siguiente hipótesis:

**H1:** *El modelo de gobierno y el apoyo de la alta gerencia afectan positivamente la detección interna de eventos de seguridad digital (ataques exitosos y no exitosos) por parte del banco.*

## 2.2 BUENAS PRÁCTICAS EN GESTIÓN DE TI / SEGINFO

En este aparte se reúne la revisión de la literatura académica relacionada con prácticas tecnológicas y administrativas adoptadas por las organizaciones con el propósito específico de mejorar de alguna forma su gestión de TI y Seginfo. Se excluyen explícitamente las prácticas dirigidas directamente a los empleados, para mejorar su desempeño en el frente de Seginfo; este tema ha sido tratado tan ampliamente en la literatura, que amerita una sección independiente en este trabajo. (Ver sección 3.3).

El informe de la OEA recoge datos sobre las siguientes prácticas: tercerización de actividades relacionadas con Seginfo, adopción de estándares internacionales en TI / Seginfo, implementación de herramientas tecnológicas, medidas técnicas, procesos y controles para la gestión de Seginfo, desarrollo de estrategias para la priorización, contención, respuesta y recuperación frente a incidentes de Seginfo, aplicación de diagnósticos de madurez organizacional en la gestión de Seginfo, y existencia de planes de comunicación a clientes. Nuevamente, para este trabajo se revisó la literatura académica existente en estos temas.

### 2.2.1 ESTÁNDARES DE SEGINFO

La literatura sobre estándares, marcos de trabajo y metodologías (en adelante, estándares, por brevedad) es bastante diversa. Una buena parte de esta literatura es de naturaleza descriptiva y busca ofrecer al lector recuentos, mapeos, presentaciones abreviadas, guías de aplicación y ejercicios de contrastación con respecto a los estándares existentes, tales como ISO 27000, Cobit, COSO, entre muchos otros (Friskén, 2015; Haufe *et al.*, 2016; Hohan *et al.*, 2015; Layton, 2016; Rahman & Choo, 2015; Saint-Germain, 2005; Susanto *et al.*, 2011; Ula *et al.*, 2011), o introducciones a las organizaciones que producen o administran estos estándares (Kerti & Nyikes, 2017). Un segundo grupo es de carácter más prescriptivo y propositivo, y busca mejorar o complementar los estándares existentes para atender necesidades particulares tales como las de las PYMES (Mijnhardt *et al.*, 2016), los ambientes en la nube (Rahman & Choo, 2015; Zhang *et al.*, 2010), el enfoque a procesos (Haufe *et al.*, 2016) o calidad (Hohan *et al.*, 2015), entre otros temas.

Es interesante observar que los estudios en estos dos grupos asumen implícitamente que los estándares tienen efectos positivos sobre el desempeño

de Seginfo en las organizaciones, y proceden directamente a describir o ampliar estos estándares, sin cuestionarse acerca de su efectividad.

El tercer grupo de estudios es algo diferente, puesto que analiza los factores que inciden en la adopción e implementación de estos estándares en las organizaciones. Inspirados en una amplia tradición sobre innovaciones administrativas en los estudios organizacionales, estas investigaciones encuentran que muchas organizaciones adoptan estándares de Seginfo debido a dinámicas internas de poder (Silva *et al.*, 2016), o por razones relacionadas con presiones institucionales existentes en su entorno, y no propiamente por expectativas de efectividad o de mejora en su desempeño (Albuquerque & Marques dos Santos, 2015; Alkalbani *et al.*, 2017). Sin embargo, otro estudio precisa estos hallazgos al reconocer que cuando las organizaciones perciben que las prácticas que su entorno les quiere imponer no son útiles para ellas, optan por eludir y desafiar dichos estándares, en lugar de adoptarlos (Hou *et al.*, 2018), con lo cual se podría inferir que las organizaciones solo adoptan estándares de Seginfo si hay presión de su entorno por hacerlo y además ellas consideran que dichos estándares pueden resultarles útiles. Entre los factores que facilitan la implementación de estándares se encuentran las competencias en TI de los gerentes de línea y la experiencia del sector en temas de Seginfo (Chang & Ho, 2006).

El cuarto y último grupo es con certeza el más relevante para nuestro trabajo, ya que hace un análisis crítico de los estándares, destacando sus fortalezas y debilidades. Entre las fortalezas encontradas se menciona que los estándares existentes son exhaustivos y sus dimensiones atienden aspectos relevantes de la gestión de Seginfo (lit1\_6). Lamentablemente, son de mayor cuantía y envergadura las debilidades encontradas. Entre las principales debilidades se ha argumentado que son excesivamente amplios y complejos para ser implementados en organizaciones pequeñas (Mijnhardt *et al.*, 2016), que contienen duplicidades innecesarias (Ma & Pearson, 2005), que al ser excesivamente generales no prestan atención a las diferencias en las necesidades de las organizaciones (Siponen & Willison, 2009). Por ejemplo, un estudio encontró que muchas de las prácticas incluidas en estos estándares eran sub-óptimas o incluso contraproducentes para organizaciones muy grandes (Jeong *et al.*, 2019).

También se ha criticado que los estándares son excesivamente abstractos, ya que solo les indican a las organizaciones “qué” trabajo deben hacer, pero no “cómo” ni “cuán bien” deben hacerlo, con lo cual terminan por

desatender un punto central en la gestión de Seginfo, y corren el riesgo de ser implementados de manera maquinal o ritualista, sin contribuir sustancialmente al logro de los objetivos propuestos (Siponen, 2006). Sumado a lo anterior, se ha discutido que la implementación de estándares puede desestimular la improvisación en respuesta a ataques, la cual ha demostrado ser un complemento necesario para lograr respuestas exitosas (McLaughlin & Gogan, 2018), y que la difusión de los estándares puede crear nuevos riesgos de Seginfo en situaciones específicas, por ejemplo, si un estándar de amplia difusión recomienda una configuración específica de software, dicha configuración se vuelve más vulnerable a ataques (McLaughlin & Gogan, 2018).

Desde una óptica más academicista, se han hecho tres críticas importantes: los estándares existentes no están basados en teoría (Ma & Pearson, 2005), no consideran la naturaleza social de los problemas que derivan en riesgos de Seginfo (Ma & Pearson, 2005), y no siguen procesos de validación rigurosa (Siponen & Willison, 2009). Esta última crítica es particularmente pertinente para nuestro trabajo, ya que advierte que la efectividad de estos estándares para mejorar la gestión de Seginfo no ha sido validada empíricamente, sino que simplemente estos estándares se asumen como válidos apelando a la autoridad de quien lo emite y al hecho de que son de usanza común. La crítica argumenta que una práctica común no es necesariamente una mejor práctica, y que haría falta evidencia empírica de los resultados de aplicar dicha práctica antes de llamarla “mejor práctica” e incluirla en un estándar.

### 2.2.2 OTRAS PRÁCTICAS ORGANIZACIONALES PARA LA GESTIÓN DE SEGINFO

Al inicio de la sección 3.2 se mencionó que el informe de la OEA recoge datos sobre varias prácticas organizacionales orientadas a la gestión de Seginfo. La sección 3.2.1 se concentró en una sola de estas prácticas: la adopción de estándares internacionales en Seginfo, dada la abundancia de literatura en este tema.

En esta sección se discutirá la literatura respecto a todas las otras prácticas abarcadas en el informe de la OEA, a saber: tercerización de actividades relacionadas con Seginfo, implementación de herramientas tecnológicas, medidas técnicas, procesos y controles para la gestión de Seginfo, desarrollo de estrategias para la priorización, contención, respuesta y recuperación frente a

incidentes de Seginfo, aplicación de diagnósticos de madurez organizacional en la gestión de Seginfo, y existencia de planes de comunicación a clientes.

Respecto a la tercerización de las actividades relacionadas con Seginfo se han estudiado las motivaciones de las organizaciones para tercerizar y algunas de las consecuencias de hacerlo. En cuanto a las motivaciones, se ha encontrado que las explicaciones convencionales de la tercerización de TI, primordialmente precio y calidad, son válidas aquí también, pero que además en la tercerización de Seginfo se busca también reducir el riesgo de ser víctima de ataques simultáneos a varias organizaciones (Cezar *et al.*, 2017). En cuanto a las consecuencias, se ha visto que la tercerización puede ser efectiva para disminuir los eventos adversos de Seginfo, siempre y cuando se planteen requerimientos altos al proveedor (Hui *et al.*, 2012) y se negocien contratos que incluyan recompensas y castigos asociados a la detección y a la responsabilidad en la ocurrencia de los eventos (Cezar *et al.*, 2014). La tercerización a múltiples proveedores también puede mejorar el desempeño de Seginfo cuando la organización asegura la colaboración entre dichos proveedores entre sí y con los proveedores de TI (Naicker & Mafaiti, 2019). Lo anterior indica que el simple hecho de tercerizar actividades de Seginfo no necesariamente genera efectos positivos sobre el desempeño, sino que es la tercerización cuidadosa la que puede traer resultados positivos.

No se encontró mucha literatura sobre la implementación de herramientas tecnológicas, medidas técnicas, procesos y controles de Seginfo. Dos estudios diferentes descubrieron que la implementación de múltiples herramientas tecnológicas puede generar efectos contrarios a los esperados, es decir, aumentar la exposición a riesgos de Seginfo, cuando varias tecnologías interdependientes no son configuradas correctamente (Cavusoglu *et al.*, 2009, Zhao *et al.*, 2015). En cuanto al tema de controles, la literatura consultada es de naturaleza prescriptiva, y sugiere recomendaciones metodológicas para optimizar los controles según varios factores contextuales, tales como las vulnerabilidades de cada organización (Almeida & Respício, 2018), la probabilidad de los ataques (Zhang *et al.*, 2018), o los costos de recuperación (Al-Safwani *et al.*, 2018). Sin embargo, esta literatura no parece haber estudiado la efectividad de implementar controles para mejorar la gestión de Seginfo.

Nuevamente, sobre los temas de estrategias de Seginfo, aplicación de diagnósticos de madurez, y existencia de planes de comunicación se identificaron relativamente pocos artículos, y parte de lo escrito parece estar

inmerso en la literatura de estándares descrita arriba. Un tema relacionado que se discute más ampliamente en la literatura es el de la formulación e implementación de políticas de Seginfo en las organizaciones. A este respecto, es importante precisar que aunque no existe un consenso en la literatura sobre qué se entiende por política ni que funciones debe abarcar una política (Paananen *et al.*, 2020), sí hay un entendimiento generalizado de que la política de Seginfo debe alinearse con la estrategia de la organización, sirve un propósito de direccionamiento de las actividades de Seginfo, y ejerce una función de comunicación dentro de la organización (Paananen *et al.*, 2020). En algunos contextos se ha identificado que pocas compañías cuentan con una política formalmente formulada, como por ejemplo en Europa del Este (Osmanbegović *et al.*, 2017), África (Arhin & Wiredu, 2018) y en empresas PYME del Reino Unido (Choi *et al.*, 2018). Solamente se identificó un estudio que investiga los efectos de tener una política de Seginfo, y este encontró que las tasas de ocurrencia de eventos adversos y el nivel de severidad de dichos eventos son iguales para las empresas que tienen una política de Seginfo implementada y para las que no la tienen (Doherty & Fulford, 2005).

Por todo lo anterior, se hace pertinente validar empíricamente, en el marco de este estudio, si la adopción de estándares y otras prácticas por parte de los bancos estudiados contribuye a la obtención de resultados positivos en materia de gestión de Seginfo, para lo cual se formuló la siguiente hipótesis:

*H2: La aplicación de buenas prácticas en la gestión de TI/Seginfo afecta positivamente la detección interna de eventos de seguridad digital (ataques exitosos y no exitosos) por parte del banco.*

### 2.3 GESTIÓN DE PERSONAL

Los temas relacionados con gestión de personal en torno a Seginfo parecen ser la mayor preocupación de los académicos en esta área. De hecho, estos estudios conforman un cuerpo temático particular, conocido en la literatura como Seginfo comportamental. La preocupación por el comportamiento humano es explicable, dado que la evidencia acumulada a lo largo de los años sugiere que las políticas, la comunicación, el entrenamiento, y otras medidas encaminadas a lograr comportamientos idóneos en materia de Seginfo por parte de los empleados resultan insuficientes para lograr que las personas alineen su comportamiento con las expectativas de la organización. Para ilustrar esta situación, se puede considerar el siguiente ejemplo: por tres

años, entre 2015 y 2018, cerca de seis mil empleados del sector de salud en los Estados Unidos recibieron un entrenamiento intensivo e integral para que supieran cómo actuar ante ataques de *phishing* por correo electrónico. Sin embargo, finalizado el entrenamiento, un estudio encontró que las personas entrenadas cometían el mismo número de equivocaciones frente a estos ataques que aquellos que no se habían entrenado (Gordon *et al.*, 2019). Un problema similar se identificó puntualmente en un estudio realizado en el sector bancario: allí, luego de recibir entrenamiento los empleados decían saber qué debían hacer, pero su comportamiento no reflejaba la puesta en práctica de dicho conocimiento (Bauer *et al.*, 2013).

Ante esta evidencia, la literatura en Seginfo comportamental se ha concentrado en estudiar los factores que explican el cumplimiento o incumplimiento de las políticas de Seginfo por parte de los empleados, las palancas que pueden usarse para elevar el nivel de conciencia de los empleados, y los mecanismos que pueden ayudar a lograr un mejor y mayor cumplimiento de las políticas de Seginfo por parte de los empleados. En este contexto, se entiende como conciencia la comprensión que tienen los empleados tanto de la importancia de actuar conforme a la política, como de las consecuencias de no hacerlo (Chmura, 2017).

Esta literatura ha explorado diversas teorías y constructos provenientes primordialmente de la psicología, buscando aplicarlos a las particularidades del contexto de Seginfo; entre los principales fundamentos teóricos se encuentran la teoría general de la disuasión (TGD), la teoría de la motivación de protección (TMP), las teorías cognitivas y la teoría de la neutralización (Crossler *et al.*, 2013).

TGD ha sido una de las teorías motivacionales más ampliamente utilizadas (p. ej., Cuganesan *et al.*, 2018; Herath & Rao, 2009; Ifinedo, 2016; Pahlila *et al.*, 2007; Siponen, 2000); esta teoría estudia la incidencia de motivadores extrínsecos, particularmente premios y castigos, sobre el comportamiento de las personas. Proveniente de la criminología, esta teoría postula que la severidad de un castigo y la probabilidad percibida de ser atrapado influyen en el comportamiento individual (Chen *et al.*, 2018). Lamentablemente, en Seginfo, los hallazgos basados en esta teoría son inconcluyentes.

Por su parte, TMP propone que las personas que las personas buscan protegerse de las amenazas existentes en su entorno, y para ello consideran tanto la severidad y probabilidad de dichas estas amenazas, como su propia vulnerabilidad a las mismas (Lee *et al.*, 2016). Si bien esta teoría ha sido

usada ampliamente en los estudios comportamentales de Seginfo (Bulgurcu *et al.*, 2010; Menard *et al.*, 2017; Pahnla *et al.*, 2007; Siponen *et al.*, 2014), los hallazgos también han sido inconsistentes (Menard *et al.*, 2017).

Otras teorías de corte más cognitivista también han sido empleadas en el contexto de Seginfo. Siguiendo la lógica de la teoría de la acción razonada (Fishbein, 1967) y su derivada, la teoría del comportamiento planeado (Ajzen, 1991), se ha postulado que la actitud frente a la política de Seginfo predice la intención de actuar conforme a la política (Aurigemma & Mattson, 2017). A su vez, estas teorías sostienen que la actitud se construye a partir de un proceso racional en donde el individuo evalúa los beneficios y los costos o esfuerzos de cumplir con la política (Kajtazi *et al.*, 2018). En la conformación de estas actitudes, se sabe que influyen las creencias personales, las normas sociales y la percepción de control, es decir, la presencia de condiciones que faciliten la realización del comportamiento (Bauer & Bernroider 2017; Bulgurcu *et al.*, 2010; Cuganesan *et al.*, 2018; Dang-Pham *et al.*, 2017a; Herath & Rao, 2009; Hu *et al.*, 2012; Humaidi *et al.*, 2018; Ifinedo, 2016; Pahnla *et al.*, 2007; Siponen *et al.*, 2014).

Dentro de los estudios de fundamentación cognitivista se han hecho importantes descubrimientos específicos para mejorar el nivel de cumplimiento de la política de Seginfo por parte de los empleados. Entre estos descubrimientos, cabe resaltar los siguientes: las políticas centralizadas contribuyen a evitar conflictos de valores en la práctica, favoreciendo el cumplimiento de la política (Karlsson *et al.*, 2018); los procesos de Seginfo, por su mecanicidad, suelen tornarse tediosos para algunos empleados, generando fatiga o estrés (D'Arcy & Teh, 2019), y cuando esto sucede los empleados pierden interés en el cumplimiento de la política (Hwang & Cha, 2018; Pham *et al.*, 2019); las prácticas organizacionales que promueven la socialización del conocimiento y las experiencias favorecen el cumplimiento de la política de Seginfo (Arhin & Wiredu, 2018; Choi *et al.*, 2018; Dang-Pham *et al.*, 2017b; Han *et al.*, 2017; He & Johnson, 2017; Karlsson *et al.*, 2017; Kim & Han, 2019; Korte, 2017; Sommestad, 2018) y han sido incluso asociadas a la reducción en la ocurrencia de eventos adversos de Seginfo (Gal-Or & Ghose, 2005). Finalmente, percepciones positivas como el empoderamiento y el sentido de pertenencia, logrados a través de la participación activa de los trabajadores en Seginfo, promueven el cumplimiento de la política de Seginfo (Balozian *et al.*, 2019; Chen *et al.*, 2019; Choi & Song, 2018; Doherty & Tajuddin, 2018; Kim & Han, 2019; Rocha-Flores & Ekstedt 2016; Yazdanmehr & Wang, 2016).

Un aporte destacado dentro de los estudios cognitivistas fue la introducción de la teoría de la neutralización, la cual estudia los diferentes tipos de argumentos que usan las personas para incurrir en comportamientos que se desvían de lo que ellos mismos consideran correcto. Estos argumentos, conocidos generalmente como ‘racionalizaciones’ o ‘técnicas de neutralización’, le permiten a la persona invalidar temporalmente sus creencias y justificar su comportamiento en contra de las mismas, sin que se genere culpabilidad o carga emocional negativa por el incumplimiento (Bauer & Bernroider, 2017; Njenga & Jordaan, 2016; Siponen & Vance, 2010). Por ejemplo, un empleado que conoce la política de Seginfo y cree que es favorable cumplirla puede decidir en una situación particular violar la política, racionalizando que la excepción es justificable por una razón personal, o porque la consecuencia de la violación es mínima. Evidentemente, si la neutralización ocurre frecuentemente, el incumplimiento puede terminar por extenderse a toda la organización.

Apalancados en la teoría de la neutralización, estudios más recientes han explorado cómo pueden las organizaciones actuar para prevenir el uso de técnicas de neutralización por parte de los empleados, y han visto que incorporar dentro de la educación y sensibilización en Seginfo un enfoque comunicativo enfocado a evidenciar e inhibir dichas técnicas, arroja buenos resultados (Barlow *et al.*, 2018, Herath *et al.*, 2018). Este tipo de comunicación enfatiza que la ética de la Seginfo no puede ser situacional, ni puede condicionarse, sino que los empleados deben en todos los casos seguir los cursos de acción recomendados por la política de Seginfo vigente.

También son importantes los estudios que evidencian que cuando los valores o creencias entran en conflicto, el trabajador puede optar por incumplir la política de Seginfo. Por ejemplo, Karlsson y sus colegas (2018) encontraron que cuando el valor de la eficiencia en el trabajo entra en conflicto con el cumplimiento de la política de Seginfo, los empleados suelen preferir el primero al segundo.

Otra fuente importante de teoría para estudiar los factores que explican el cumplimiento o incumplimiento de la política de Seginfo por parte de los empleados se halla en los estudios de cultura organizacional. La cultura se define como programación colectiva de la mente que distingue unos grupos sobre otros (Sommestad, 2018). En el contexto de Seginfo, se dice que la cultura se genera y fortalece mediante la interacción de las personas entre sí y con los procedimientos y controles (Nel & Drevin, 2019). Numerosos

estudios han encontrado que la cultura organizacional (Hu *et al.*, 2012; Humaidi *et al.*, 2018; Ifinedo, 2016), la percepción de obligatoriedad de la política (Boss *et al.*, 2009), y la identificación del personal con la misión de la organización (Choi *et al.*, 2018) contribuyen de manera importante al cumplimiento de la política de Seginfo por parte de los empleados. Y en contraposición, comportamientos o atributos individuales negativos tales como la adicción a Internet o el uso de los computadores del trabajo con fines personales, se han asociado empíricamente al incumplimiento de la política de Seginfo (Hadlington & Parsons, 2017).

En tiempos recientes, los estudios comportamentales de Seginfo han diversificado su base teórica, multiplicando así la cantidad de teorías provenientes de la psicología, tales como la teoría del autocontrol (Hu *et al.*, 2015, West *et al.*, 2019), la teoría de la autodeterminación (Menard *et al.*, 2017), la teoría de la resistencia reactiva (Lowry & Moody, 2015; Lowry *et al.*, 2015), o la teoría de la justicia (Lowry *et al.*, 2015), la criminología, tales como la teoría de la oportunidad criminal (Wang *et al.*, 2019), y la psicología social, tales como la teoría de la desorganización social (Johnston *et al.*, 2019), que dan fundamento a las explicaciones del comportamiento de los empleados frente a la Seginfo.

Sin embargo, las revisiones agregadas hechas sobre esta abundante literatura no son alentadoras. Una revisión sistemática de la literatura en Infoseg comportamental, publicada en 2014, examinó 29 estudios, los cuales contenían más de 60 variables, y llegó a la conclusión de que no existe un conjunto de variables ni de teorías que logren explicar de manera robusta el comportamiento de los empleados en Infoseg, y de hecho encontró que los resultados de las mismas variables en distintos estudios son muchas veces inconsistentes entre sí (Sommestad *et al.*, 2014). Otro estudio, esta vez un metaanálisis (Cram *et al.*, 2019), exploró los resultados para cada una de las teorías clásicas en el tema (TGD, TMP, teorías cognitivas), y encontró nuevamente que ninguna de ellas puede demostrar superioridad empírica sobre las otras, y concluyó que ello “resume de manera general el estado de la situación en la literatura sobre el cumplimiento de políticas de Infoseg: hay una falta de consenso en cuanto a los factores que inciden en el cumplimiento de la política, e incertidumbre acerca de cómo estos factores actúan bajo diferentes condiciones” (Cram *et al.*, 2019, p. 549).

No obstante lo anterior, este último estudio identificó que las variables intrínsecas al individuo, tales como su ética, sus valores y creencias, y sus actitudes, son las que tienen mayores efectos y muestran mayor regularidad

a la hora de predecir el comportamiento de los empleados en materia de cumplimiento a las políticas de Seginfo, y en consecuencia, los autores del estudio son enfáticos en afirmar que para que las empresas logren un buen comportamiento por parte de sus empleados, deben concentrarse en identificar a las personas correctas en sus procesos de selección, para contratarlas. El estudio también encontró que las variables menos útiles para predecir comportamiento son las relacionadas con motivación extrínseca, es decir, las recompensas y los castigos, y que las variables asociadas con el entrenamiento tienen un efecto moderado sobre el comportamiento (Cram *et al.*, 2019).

Por último, es importante destacar una crítica hecha por varios autores: una característica frecuente de los estudios de Infoseg comportamental es usar como variable a observar *la intención* de los empleados de cumplir la política, y no *el comportamiento* propiamente dicho, lo cual resulta inadecuado dado que en el contexto de Infoseg es muy usual que el comportamiento real no corresponda a la intención (Cram *et al.*, 2019; Crossler *et al.*, 2003).

Con el fin de validar empíricamente si las medidas de gestión de personal reportadas por los bancos cubiertos en el estudio de la OEA contribuyen a la obtención de resultados positivos en materia de gestión de Seginfo, se formuló la siguiente hipótesis:

*H3: La buena gestión de personal en asuntos relacionados con Seginfo afecta positivamente la detección interna de eventos de seguridad digital (ataques exitosos y no exitosos) por parte del banco.*

## 2.4 IMPACTO DE LOS ATAQUES

Para esta revisión se pretendió localizar literatura relacionada con ocurrencia de eventos de seguridad, detección de estos y su impacto económico para las organizaciones que los sufren.

Lamentablemente, no fue posible identificar artículos que exploraran la relación entre la ocurrencia y la detección interna de eventos. Dado que el informe de la OEA incluye información sobre ambos temas, para este estudio sí se pudo explorar esta relación. Esto se hizo asumiendo que la detección interna de eventos desincentiva a los atacantes, y por consiguiente puede ayudar a contener o disminuir su ocurrencia, lo cual lleva a formular la siguiente hipótesis:

*H4: La detección interna de eventos de seguridad digital (ataques exitosos y no exitosos) por parte del banco afecta favorablemente (disminuye) la ocurrencia de eventos de seguridad digital (ataques exitosos y no exitosos) dirigidos al banco.*

Contrariamente, la literatura académica sí explora el impacto económico causado por los eventos de Seginfo de que son víctimas las organizaciones. Para medir el impacto económico, los estudios revisados han usado variables relacionadas con el desempeño de la acción de las empresas afectadas en el mercado de valores. En general, los estudios publicados han encontrado que los ataques afectan negativamente el valor de las acciones (p. ej.: Berkman *et al.*, 2018; Gordon *et al.*, 2011, Schatz & Bashroush, 2016) y que dicho efecto puede tener repercusiones de largo plazo (Hinz *et al.*, 2015). En una revisión sistemática de 45 estudios publicados sobre el tema entre 1988 y 2012, Spanos y Angelis (2016) notaron que el 76 % de estos estudios identifican una disminución en el precio de la acción tras la ocurrencia de ciberataques. Sin embargo, también se ha visto que el impacto de los ciberataques sobre el valor de la acción ha venido cediendo en el tiempo; algunos autores interpretan esta tendencia como una normalización de los ciberataques, y postulan entonces que estos ataques deben entenderse ahora como un costo operativo de hacer negocios en la era digital (Gordon *et al.*, 2011; Yayla & Hu, 2011).

Algunos estudios han explorado factores contextuales que afectan el impacto económico sufrido por las organizaciones víctimas. Se ha encontrado que los tipos de ataques que parecen ser más nocivos son aquellos que dan acceso indebido a información confidencial (Gordon *et al.*, 2011; Jeong *et al.*, 2019), afectan la disponibilidad de los servicios de TI y la información (Whitman, 2004; Yayla & Hu, 2011), y también que los ataques repetitivos generan un impacto negativo creciente (Schatz & Bashroush, 2016).

Continuando con los factores de entorno, se ha identificado que las empresas de comercio electrónico son tres veces más propensas a recibir ataques (Yayla & Hu, 2011), que otros sectores particularmente afligidos por las consecuencias económicas de los ciberataques incluyen el financiero (Jeong *et al.*, 2019), que los sectores de hidrocarburos y textiles son particularmente vulnerables puesto que presentan unos bajos niveles de Seginfo (Berkman *et al.*, 2018). También se ha visto que la forma en que los medios comunican la gravedad del evento de Seginfo afecta significativamente la consecuencia económica de este, y por lo tanto la capacidad de recuperación de la empresa (Tsohou *et al.*, 2015).

Una línea complementaria de investigación ha explorado el impacto económico ya no de los ataques, sino de la gestión proactiva en Seginfo. Se ha encontrado, por una parte, que el mercado premia la inversión preventiva en Seginfo con incrementos en el valor de la acción (Chai *et al.*, 2011) y, por

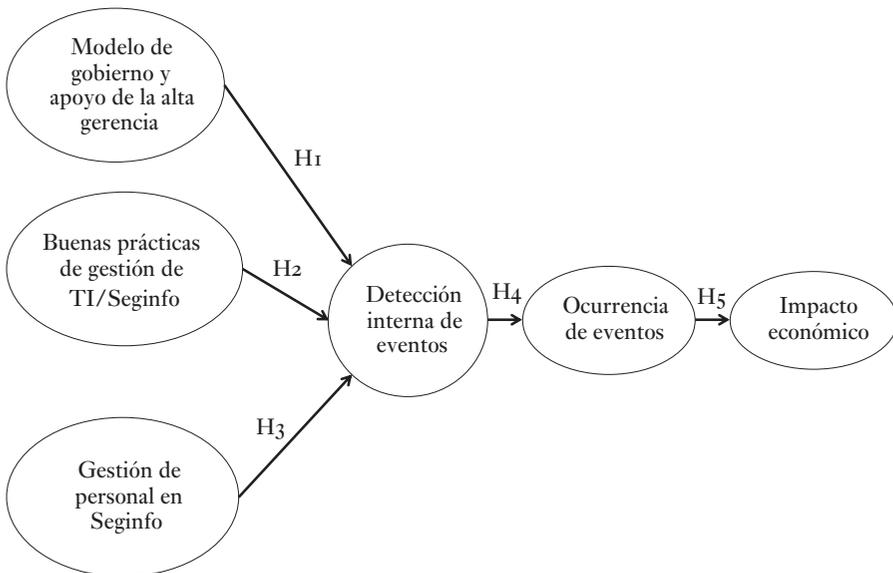
otra, que el trabajo de la organización en implementar políticas de Seginfo (Chai *et al.*, 2011; Whitman, 2004; Wu *et al.*, 2015) y concientizar a los empleados acerca del importante rol que juegan en una gestión efectiva de Seginfo (Berkman *et al.*, 2018; Hinz *et al.*, 2015) resulta ser un mecanismo efectivo para disminuir el impacto económico de los ataques.

Lo anterior hace que se plantee la siguiente hipótesis:

*H5: La ocurrencia de eventos de seguridad digital (ataques exitosos y no exitosos) dirigidos al banco afecta negativamente (aumenta) el impacto económico de los eventos de seguridad digital (ataques exitosos y no exitosos) dirigidos al banco.*

En resumen, el modelo plantea cinco hipótesis como se observa en la figura 1.

FIGURA 1. MODELO DE INVESTIGACIÓN



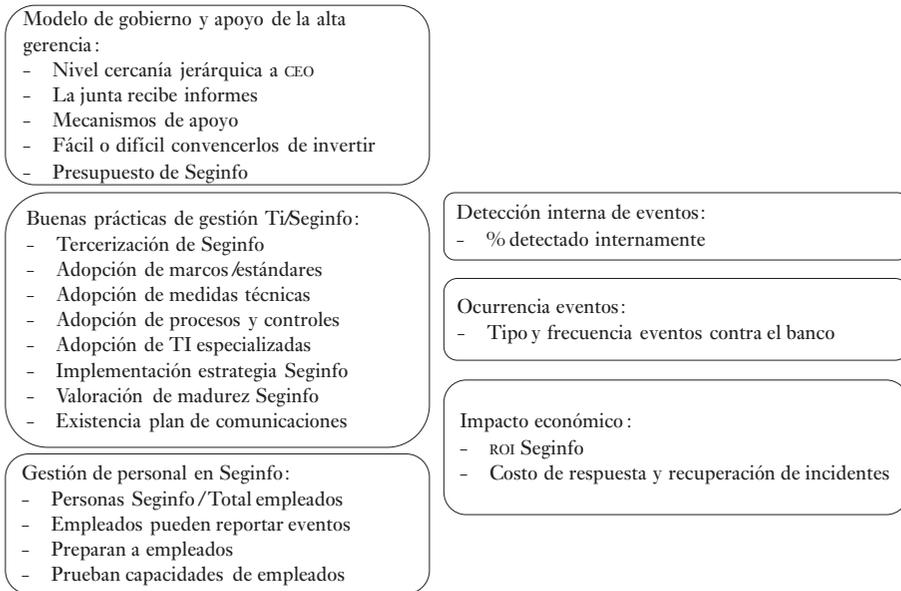
Fuente: los autores.

### 3. METODOLOGÍA

Como ya fue mencionado, este capítulo tomó los datos maestros levantados sobre 191 bancos de la región para el mencionado estudio de la OEA. Estos datos fueron agrupados en seis constructos, los cuales recogen preguntas

relacionadas con dichos constructos en el estudio de origen, según se muestra en la figura 2.

FIGURA 2. TEMAS EXPLORADOS EN LOS CONSTRUCTOS DEL PRESENTE ESTUDIO



Fuente: los autores.

En el estudio original de la OEA, las preguntas están planteadas como variables categóricas, es decir, el participante debía escoger una o varias opciones de respuesta de una lista de textos descriptivos. Entonces, para construir constructos susceptibles de medición estadística, fue necesario convertir las opciones de respuesta originales a escalas numéricas discretas. En el anexo 1 se presentan los detalles sobre esta conversión.

Esos seis constructos fueron modelados en una ecuación estructural, y analizados con el método de regresión de los mínimos cuadrados parciales (*partial least squares*, en inglés), usando el software SmartPLS versión 3.0. El análisis de los datos sigue los preceptos indicados para ecuaciones estructurales de manera general, y para el método escogido en particular, con lo cual se hace primero una valoración del modelo de medición y luego una valoración del modelo estructural, para corroborar las hipótesis formuladas. Dichos análisis se presentan en la siguiente sección.

## 4. RESULTADOS

## 4.1 VALORACIÓN DEL MODELO DE MEDICIÓN

Para valorar la validez del modelo de medición, se tuvieron en cuenta cuatro atributos de validez de los constructos del modelo, a saber: confiabilidad de los ítems individuales, consistencia interna, validez convergente y validez discriminante. Todos los constructos multi-ítem fueron modelados como constructos reflectivos, de manera que la valoración siguió el mismo procedimiento para todos ellos.

Para medir la confiabilidad de los ítems individuales, se tomaron las cargas externas (*outer loadings*) de cada ítem con su respectivo constructo. Se retiraron de cada constructo aquellos ítems con cargas inferiores a 0,6. La tabla I presenta los ítems retenidos para cada constructo con los valores de sus cargas externas.

TABLA I. CONFIABILIDAD DE ÍTEMS INDIVIDUALES, ÍTEMS RETENIDOS

Constructo	Sigla	N.º ítem	Nombre ítem	Carga externa
Modelo de gobierno y apoyo de la alta gerencia	AAG	3	Manifestaciones apoyo alta gerencia	0,855
		4	Complejidad convencer alta gerencia de invertir	0,617
		5	Presupuesto	0,789
Buenas prácticas de gestión de TI/Seginfo	BP	2	Marcos / estándares internacionales	0,663
		3	Acciones y medidas técnicas	0,896
		4	Sistemas	0,855
		5	Procesos	0,857
Gestión de personal en Seginfo	GP	2	Mecanismos ofrecidos a empleados para reportar incidentes	0,915
		3	Planes de preparación, respuesta y capacitación a empleados	0,628
Detección interna de eventos	DE	1	% eventos detectados	N. A.

Constructo	Sigla	N.º ítem	Nombre ítem	Carga externa
Ocurrencia de eventos	OE	1	Ingeniería social	0,764
		2	Código malicioso o <i>malware</i>	0,762
		3	<i>Phishing</i> dirigido a sistemas del banco	0,707
		5	Pérdida o robo de equipos o dispositivos	0,616
		10	Fraude interno	0,634
Impacto económico	IE	2	Costo respuesta y recuperación	N. A.

Para valorar la consistencia interna, se revisaron los índices de confiabilidad compuesta generados por SmartPLS 3.0. Allí se espera que todos sean mayores de 0,7, lo cual se cumplió en este caso, como se muestra en la tabla 2.

TABLA 2. CONSISTENCIA INTERNA

Constructo	Índice de confiabilidad compuesta ( <i>composite reliability</i> )
Modelo de gobierno y apoyo de la alta gerencia	0,801
Buenas prácticas de gestión de TI/Seginfo	0,892
Gestión de personal en Seginfo	0,756
Detección interna de eventos	1,000
Ocurrencia de eventos	0,826
Impacto económico	1,000

Para valorar la validez convergente, se revisaron los índices de varianza extraída media (*average variance extracted*, AVE) generados por SmartPLS 3.0. Allí se espera que todos sean mayores de 0,5. En la tabla 3 se muestra que solo un constructo tuvo un AVE ligeramente por debajo de 0,5.

TABLA 3. VALIDEZ CONVERGENTE

Constructo	AVE
Modelo de gobierno y apoyo de la alta gerencia	0,578
Buenas prácticas de gestión de TI/Seginfo	0,677

Constructo	AVE
Gestión de personal en Seginfo	0,616
Detección interna de eventos	1,000
Ocurrencia de eventos	0,489
Impacto económico	1,000

Finalmente, para valorar la validez discriminante se revisó que las cargas de cada ítem fueran mayores en su propio constructo que en otros constructos, lo cual se puede constatar en la tabla 4, que contiene todas las cargas de los ítems retenidos en el modelo.

TABLA 4. VALIDEZ DISCRIMINANTE

Constructo	ONP	AAG	BP	GP	DE	OE	IE
AAG, ítem 3	0,113	0,855	0,494	0,286	0,274	-0,203	0,036
AAG, ítem 4	0,027	0,617	0,334	0,154	0,124	0,076	0,060
AAG, ítem 5	0,195	0,789	0,306	0,246	0,258	-0,125	0,007
BP, ítem 2	0,077	0,325	0,663	0,287	0,251	-0,256	-
BP, ítem 3	0,293	0,440	0,896	0,314	0,443	-0,172	-0,071
BP, ítem 4	0,352	0,386	0,855	0,338	0,378	-0,224	-0,081
BP, ítem 5	0,168	0,483	0,857	0,364	0,404	-0,063	0,006
GP, ítem 2	0,149	0,219	0,312	0,915	0,247	-0,034	0,057
GP, ítem 3	-0,007	0,326	0,337	0,628	0,128	-0,031	0,056
DIE	0,294	0,305	0,459	0,253	1,000	-0,261	-0,094
OE, ítem 1	-0,064	-0,122	-0,095	-0,004	-0,201	0,764	0,183
OE, ítem 2	-0,147	-0,163	-0,165	0,002	-0,123	0,634	0,142
OE, ítem 3	-0,162	-0,065	-0,113	-0,076	-0,280	0,762	0,159
OE, ítem 5	-0,154	-0,061	-0,170	-0,029	-0,092	0,707	0,151
OE, ítem 10	-0,169	-0,090	-0,181	-0,018	-0,151	0,616	0,182
IE, ítem 2	-0,126	0,037	-0,053	0,069	-0,094	0,234	1,000

## 4.2 VALORACIÓN DEL MODELO ESTRUCTURAL

Luego de depurado el modelo y valorados sus atributos de medición, se procedió a realizar un análisis del modelo estructural para verificar las hipótesis. Para ello, se hizo una corrida del modelo con la técnica de *bootstrapping*. Los resultados se presentan en la tabla 5.

TABLA 5. VALIDACIÓN DE HIPÓTESIS

N.º	Hipótesis	T stat.	P val.	Resultado
H1	Apoyo alta gerencia --> Detección interna eventos	1,113	0,266	Rechazada
H2	Buenas prácticas --> Detección interna eventos	5,076	0,000	Confirmada
H3	Gestión de personal --> Detección interna eventos	1,083	0,279	Rechazada
H4	Detección interna eventos --> Ocurrencia eventos	3,390	0,001	Confirmada
H5	Ocurrencia eventos --> Impacto económico	2,436	0,015	Confirmada

Las hipótesis 2, 4 y 5 fueron confirmadas.

Respecto a la hipótesis 2, se encontró que los bancos que han adoptado un mayor número de buenas prácticas con respecto a la gestión de TI y Seginfo son aquellos que tienen mejores resultados en cuanto a su detección interna de eventos de Seginfo mediante sistemas propios.

La confirmación de la hipótesis 4 significa que los bancos que obtienen mejores resultados en cuanto a su detección interna de eventos de Seginfo, son también aquellos que reportan una menor frecuencia en la ocurrencia de los diferentes eventos de Seginfo contra el banco.

La confirmación de la hipótesis 5 significa que los bancos que reportan una menor frecuencia en la ocurrencia de los diferentes eventos de Seginfo, reportan también un menor impacto económico adverso, particularmente unos menores costos de respuesta y recuperación ante incidentes (ataques exitosos) en seguridad digital.

Por su parte, las hipótesis H1 y H3 fueron rechazadas.

Respecto a la hipótesis 1, no se encontró que los bancos que demuestran un mayor apoyo de la alta gerencia muestren mejores resultados en cuanto a su detección interna de eventos de Seginfo mediante sistemas propios.

Finalmente, el rechazo de la hipótesis 3 significa que los bancos que demuestran una mejor gestión de personal en temas relacionados con Seginfo

no obtienen mejores resultados en cuanto a su detección interna de eventos de Seginfo mediante sistemas propios.

Si bien estos dos últimos resultados van en contravía de la expectativa general y de las recomendaciones existentes sobre el tema por parte de expertos en Seginfo en la industria de TI, son en parte explicables a la luz de las discusiones académicas existentes, enunciadas previamente en este documento. Por esto, en la siguiente sección serán explorados en mayor detalle.

#### 4.3 ANÁLISIS DE SENSIBILIDAD DEL MODELO ESTRUCTURAL

Al modelo se le buscaron incluir algunas variables de control, correspondientes a otros factores que pudieran incidir en los diferentes constructos y relaciones planteados en las hipótesis anteriores. Se consideraron como posibles variables de control el tamaño del banco, asumiendo que los bancos más pequeños presentan menos fortalezas en su gestión (apoyo de la alta gerencia, buenas prácticas en gestión de TI / Seginfo, y gestión de personal), las utilidades del banco, asumiendo esto mismo para los bancos menos rentables, y la penetración de las operaciones por canales no presenciales, tales como los cajeros electrónicos, Internet y banca móvil. En este último caso, se asumió que, a mayor penetración de los canales no presenciales en las operaciones, el banco presentaría mayores fortalezas en su gestión.

En el momento de la valoración del modelo de medición, las variables de tamaño y utilidades tuvieron que descartarse, reteniendo solamente la penetración de las operaciones por canales no presenciales. Esta variable se modeló como determinante de los tres constructos investigados en este estudio, a saber: el modelo de gobierno y el apoyo de la alta gerencia, las buenas prácticas en gestión de TI / Seginfo y la gestión de personal. La variable tiene solamente una relación significativa positiva con las buenas prácticas en gestión de TI / Seginfo, lo cual significa que los bancos con una mayor penetración de operaciones por canales no presenciales son también aquellos que presentan más avance en las buenas prácticas de gestión de TI / Seginfo.

La inclusión de esta variable no afectó la medición de los constructos ni la corroboración de las hipótesis incluidas en el modelo estructural. De hecho, las cifras reportadas arriba corresponden a las resultantes incluida esta variable.

## 5. DISCUSIÓN Y CONCLUSIONES

En esta sección se revisan y contrastan los resultados obtenidos en el presente estudio a la luz de la literatura académica estudiada, para determinar los aportes que el estudio ofrece a la comunidad académica y ofrecer algunas recomendaciones tanto a los bancos de América Latina y el Caribe, nuestros sujetos de estudio, como a la OEA, dado su interés e influencia sobre la conversación en ciberseguridad bancaria en la región.

### 5.1 MODELO DE GOBIERNO Y APOYO DE LA ALTA GERENCIA

Las dos preguntas relacionadas con gobernanza (niveles entre CEO y Seginfo, y reporte a la junta como parte del modelo de gobierno) fueron descartadas en el proceso de valoración del modelo de medición. En cambio, las tres preguntas relacionadas propiamente con apoyo de la alta gerencia (manifestaciones de apoyo, complejidad para convencer a la alta dirección de invertir y asignación de presupuesto) fueron retenidas.

Lo anterior implica que los datos del estudio de la OEA no pueden ni confirmar ni rechazar la relación entre el modelo de gobierno de Seginfo y la gestión de Seginfo, medida esta como la capacidad del banco de detectar eventos a través de sus propios sistemas.

El estudio sí pudo en cambio explorar la relación entre el apoyo de la alta gerencia y la gestión de Seginfo (medida de la misma forma); sin embargo, contrario a la hipótesis, el estudio no encontró relación significativa entre el AAG y la detección interna de eventos. Aquí es importante destacar que, si bien múltiples estudios han encontrado que el AAG contribuye a la gestión (ver sección 3.1), otros autores sostienen que no toda la literatura es concluyente respecto a los efectos positivos del apoyo de la alta gerencia sobre el desempeño en Seginfo (Cram *et al.*, 2019; Cuganesan *et al.*, 2018). Con lo cual este resultado no es sorprendente, sino que coincide con todos aquellos que no han encontrado efectos positivos.

Adicionalmente, la literatura académica ha explorado de manera más particular si el AAG incide en las actitudes de los empleados y en su cumplimiento de las políticas de Seginfo. El estudio de la OEA no mide actitudes de los empleados ni su cumplimiento de las políticas de Seginfo. Se identifican entonces dos oportunidades de mejora para futuras ediciones del

estudio de la OEA: por una parte, incluir preguntas acerca de las actitudes y comportamientos de empleados frente a Seginfo y, por otra, ampliar las preguntas relacionadas con gobernanza, dándole prioridad a preguntas que puedan someterse a estudio estadístico, para poder separar los constructos de gobernanza y apoyo de la alta gerencia.

## 5.2 BUENAS PRÁCTICAS DE GESTIÓN DE TI/SEGINFO

Para formar el constructo de buenas prácticas de gestión de TI/Seginfo, se reunieron ocho preguntas del informe de la OEA. La mitad de estos ítems, relacionados con adopción de marcos y estándares, acciones y medidas técnicas, procesos, y sistemas de información (TI) para Seginfo, pudieron ser retenidos dentro del constructo. La otra mitad, en particular aquellos relacionados con *outsourcing*, estrategia, valoración de madurez, y existencia de un plan de comunicaciones en Seginfo, tuvieron que ser descartados, pues no cumplieron los requerimientos necesarios del modelo estadístico.

Retenidos los ítems anteriores, la hipótesis formulada, según la cual la aplicación de buenas prácticas en TI y Seginfo afecta positivamente la detección interna de eventos adversos, fue corroborada.

Una implicación muy valiosa de este hallazgo es que, contrario a lo que ha dicho alguna literatura, nuestro estudio encuentra que la adopción de estándares de Seginfo sí contribuye a alcanzar un mejor desempeño en Seginfo. Específicamente, la literatura académica ha dicho que los estándares en Seginfo no atienden las particularidades de muchas organizaciones (Ma & Pearson, 2005), que son demasiado abstractos (Siponen, 2006), que pueden llevar a prácticas subóptimas (Siponen & Willison, 2009) y que sus prácticas no han sido rigurosamente validadas (Siponen & Willison, 2009). Sin embargo, las cifras de nuestro estudio indican que los bancos que han avanzado en la adopción de estándares de Seginfo muestran un mejor desempeño en una variable crítica, la cual es la detección interna de ataques. En este sentido, nuestro estudio es consistente con los hallazgos de Kwon y Johnson (2018), quienes, en el contexto del sector de salud estadounidense, encontraron que la certificación de “uso significativo” de un sistema de información estaba asociada en el largo plazo con una menor ocurrencia de eventos adversos de Seginfo. Es importante aclarar que nuestro hallazgo no puede llevarnos a concluir que ciertas prácticas o ciertos estándares en particular son más efectivos o mejores, puesto que la exploración aquí es

demasiado agregada. Para llegar a este tipo de conclusiones se necesitaría más granularidad en la información.

Una segunda implicación central de nuestro estudio es que las prácticas de índole más operativa, tales como la implementación de tecnologías, medidas técnicas, controles y procesos, parecen ser las que mejor funcionan en el momento de detectar eficazmente eventos de Seginfo. Si bien la literatura explorada advierte que las organizaciones deben tener cuidado con los posibles efectos adversos de implementar varias tecnologías interdependientes (Cavusoglu *et al.*, 2009; Zhao *et al.*, 2015), nuestros resultados indican que, a más prácticas implementadas, mejores resultados en materia de detección interna. De manera similar, nuestro estudio hace un aporte importante a la literatura, al encontrar que la aplicación de medidas y acciones técnicas sí arroja resultados positivos en cuanto a la detección interna de eventos.

Por último, las prácticas más estratégicas, como la tercerización, las valoraciones de madurez en Seginfo o los planes de comunicaciones, no pudieron incluirse en el constructo y por eso no podemos extraer inferencias al respecto. En cuanto a la tercerización, dado que la literatura ha encontrado que solo funciona cuando se hace con mucha atención al detalle, es apenas razonable que este estudio no pueda validar estas conclusiones. Recordemos que el estudio base de la OEA no exploró las variables de contexto que se han identificado como relevantes en cuanto a los resultados en la literatura académica, tales como la modalidad del contrato (Cezar *et al.*, 2014) y los requerimientos al proveedor (Hui *et al.*, 2012).

### 5.3 GESTIÓN DE PERSONAL EN SEGINFO

El constructo de gestión de personal en Seginfo reunía inicialmente cuatro preguntas del informe de la OEA. La mitad de estos ítems, los relacionados con ofrecer a los empleados mecanismos de reporte de ataques y con diseño y ejecución de planes de capacitación, se retuvieron dentro del constructo. Los otros dos tuvieron que ser descartados, pues no cumplieron los requerimientos necesarios del modelo estadístico.

Adicionalmente, la hipótesis formulada, según la cual una buena gestión de personal en Seginfo afecta positivamente la detección interna de eventos adversos, fue rechazada. Es decir, en los bancos de América Latina y el Caribe los esfuerzos en gestión de personal en materia de Seginfo no se correlacionan con el desempeño en detección interna de eventos de Seginfo.

Este resultado, aunque desalentador para la OEA y el sector bancario, no es sorprendente y se puede explicar a la luz de la literatura académica existente sobre el tema, comentada en la sección 3.3 del presente capítulo, al menos de dos maneras.

En primer lugar, la literatura en Seginfo comportamental no ha llegado aún a resultados contundentes con respecto a muchas de las prácticas en gestión de personal, de forma que no se ha comprobado si dichas prácticas son efectivas para mejorar el desempeño en Seginfo (Cram *et al.*, 2019; Sommestad *et al.*, 2014). Esto explica por qué —aunque desde la práctica profesional se crea que tener personal suficiente para el tema, ofrecer a los empleados mecanismos de reporte de ataques e implementar planes de capacitación deberían mejorar el desempeño en Seginfo— desde la academia se sepa que estos mecanismos no siempre mejoran el comportamiento de los empleados en Seginfo (p. ej., Bauer *et al.*, 2013; Gordon *et al.*, 2019).

En segundo lugar, la literatura académica sí ha identificado algunos factores que promueven o impiden el cumplimiento de la política de Seginfo por parte de los empleados. En principio, estos factores deberían entonces mejorar el desempeño en Seginfo. Sin embargo, el estudio de la OEA no recogió información sobre ninguno de estos factores. Entre los factores previamente identificados como facilitadores del cumplimiento de la política y que mejoran la gestión de Seginfo encontramos: manejar una política centralizada de Seginfo (Karlsson *et al.*, 2018), promover la socialización del conocimiento y las experiencias de los empleados (Arhin & Wiredu, 2018; Choi *et al.*, 2018; Dang-Pham *et al.*, 2017b; Han *et al.*, 2017; He & Johnson, 2017; Karlsson *et al.*, 2017; Kim & Han, 2019; Korte, 2017; Pérez-González *et al.*, 2019; Rocha-Flores & Ekstedt, 2016; Sommestad, 2018), permitir la participación activa de los trabajadores en el diseño de las políticas de Seginfo (Balozian *et al.*, 2017; Chen *et al.*, 2019; Choi & Song, 2018; Doherty & Tajuddin, 2017; Kim & Han, 2019; Yazdanmehr & Wang, 2016) y mejorar los materiales de capacitación para que contribuyan a evidenciar e inhibir el uso de técnicas de neutralización (Barlow *et al.*, 2018; Herath *et al.*, 2018). Todos estos factores, relacionados con la gestión de personal, deberían contribuir a un mejor desempeño en Seginfo, y no fueron abordados por el estudio de la OEA.

Para los bancos, la recomendación entonces es considerar la incorporación de prácticas de gestión de personal que trasciendan la simple capacitación en Seginfo e incorporen factores respaldados por evidencia empírica,

tales como los señalados en el párrafo anterior. Para la OEA en particular, dado su rol de referente y faro en el tema para los bancos de la región, es indispensable que futuras ediciones del estudio desarrollen más ampliamente las preguntas orientadas al tema de gestión de personal. En otras palabras, las preguntas incluidas en la versión de 2018 son un tanto ingenuas si se ven a la luz del avance científico en Seginfo comportamental, y la OEA puede, mediante un cuestionario más sofisticado, enviar señales al sector bancario acerca de los temas que deben ser importantes en su gestión de personal.

#### 5.4 DETECCIÓN INTERNA Y OCURRENCIA DE EVENTOS

Para efectos de este estudio, el cual correlaciona posibles variables causales relacionadas con acción gerencial en frentes como la gobernanza, la gestión humana y las buenas prácticas de TI/Seginfo, es fundamental que haya una buena correlación entre la detección interna de eventos y la ocurrencia de estos en el sentido esperado, es decir, que a mayor detección interna<sup>2</sup> haya menor ocurrencia, dado que esta correlación sugiere indirectamente que las acciones gerenciales estudiadas disminuyen la ocurrencia de eventos de Seginfo.

Por esta razón, la corroboración de la hipótesis formulada en este sentido es particularmente valiosa. Esta corroboración es además un aporte a la literatura académica, ya que en la literatura revisada no se encontraron estudios que exploraran esta relación.

---

2 Es necesario recordar al lector que el estudio de la OEA, en su pregunta sobre detección interna de ataques, señala catorce tipos de estos: ingeniería social, código malicioso o *malware*, *phishing* dirigido para tener acceso a sistemas del banco, pérdida de datos, pérdida o robo de equipos o dispositivos, ataque de negación del servicio (DoS / DDoS), robo de DNS, violación de políticas de escritorio limpio, sabotaje interno, fraude interno, *defacement*, *backdoor* (código desarrollado para habilitar acceso posterior), *SQL Injection*, y ataque de fuerza bruta. Nuevamente, en la validación estadística del modelo de medición, solo cinco de estos tipos de ataques pudieron ser retenidos en el constructo correspondiente, a saber: ingeniería social, código malicioso o *malware*, *phishing*, pérdida o robo de equipos o dispositivos y fraude interno. Esto no quiere decir que estos cinco tipos de ataques hubieran ocurrido con mayor o menor frecuencia que los otros, sino que las respuestas de frecuencia convergen más entre ellas para formar un único constructo llamado *ocurrencia*; es decir, estos cinco tipos de ataques tienen frecuencias más similares entre sí, lo cual es necesario para la medición estadística.

## 5.5 IMPACTO ECONÓMICO

Para formar el constructo de impacto económico se reunieron dos preguntas del informe de la OEA: el retorno (ROI) de las inversiones en Seginfo y el costo de respuesta y de recuperación frente a ataques exitosos. En el proceso de validación del modelo estadístico, la primera de estas preguntas tuvo que ser descartada. En consecuencia, el constructo de impacto económico corresponde solamente a los costos en que incurren los bancos tras la ocurrencia de ciberataques.

La hipótesis formulada, según la cual la ocurrencia de eventos tiene un impacto económico adverso sobre el banco, fue corroborada.

Si bien la mayoría de los estudios previos sobre el tema arrojan este mismo resultado, la corroboración de esta hipótesis en este estudio representa un aporte sustancial a la literatura, en virtud de las diferencias de medición empleadas aquí. Mientras que la literatura existente se ha concentrado en medir el impacto económico por la vía de los cambios en el precio de la acción de las compañías afectadas por los ataques (p. ej., Berkman *et al.*, 2018; Gordon *et al.*, 2011; Hinz *et al.*, 2015; Schatz & Bashroush, 2016), basados en el estudio de la OEA aquí dicho impacto se midió por medio de los costos de respuesta y recuperación estimados por los propios bancos en función de su Ebitda. Para las economías latinoamericanas, con mercados de valores menos desarrollados, en donde una porción mucho menor de compañías transa su acción en las bolsas de valores, es valioso contar con mediciones de impacto económico que no estén atadas al valor de la acción en el mercado bursátil. Además, obtener un resultado coincidente con los hallazgos de la investigación académica acumulada a lo largo del tiempo en otras geografías, ofrece confianza en la medición. Este aporte nos permite ser optimistas acerca de la pertinencia de usar medidas más inclusivas, no atadas al mercado de valores, para determinar impactos económicos en estudios organizacionales de manera más amplia.

## 5.6 CONCLUSIONES

En esta parte final se reiteran los principales aportes del estudio dirigidos a tres actores relevantes para el tema de interés: la academia, la OEA, como organismo interesado en el tema y gestor del estudio de donde se tomaron los datos aquí analizados, y los bancos de la región, como entidades

vulnerables a ataques que pongan en riesgo la información y el dinero de sus usuarios.

Para la academia este estudio hace tres aportes principales. En primer lugar, se encuentra que la adopción de estándares relacionados con Seginfo sí se encuentra asociada a un mejor desempeño en Seginfo, particularmente a una mayor detección interna de ataques por parte de los bancos de la región. Esta contribución es relevante, ya que la literatura consultada se sitúa en uno de dos extremos: confía ciegamente en el valor de estos estándares, sin cuestionarse su eficacia, o bien crítica la falta de evidencia empírica respecto a la eficacia de dichos estándares. Los datos recogidos por la OEA y analizados en este informe confirman que los bancos que han avanzado en la adopción de estándares de Seginfo tienen un mejor desempeño en esta materia.

En segundo lugar, los datos de la OEA permiten corroborar una asociación favorable entre la detección interna y la ocurrencia de eventos adversos de Seginfo, de forma que a mayor detección interna se presenta una menor ocurrencia. Esta asociación abre puertas a mayor investigación sobre el tema.

Tercero, el estudio ofrece un aporte metodológico en tanto reafirma la relación previamente estudiada entre ocurrencia de eventos adversos y resultados económicos de las organizaciones, pero lo hace no desde el valor de la acción, que, si bien es una medida adecuada y ampliamente aceptada, no es una medida que pueda usarse confiablemente en el contexto de muchas economías emergentes. En contextos en donde los mercados de valores son pequeños o inmaduros, resulta útil tener medidas de impacto económico más directas. El estudio de la OEA recurrió al reporte de costos incurridos por parte de los encuestados, y esta medida arrojó resultados equivalentes a los obtenidos previamente usando como medida el valor de la acción.

Se hacen algunas recomendaciones a la OEA, todas relacionadas con el cuestionario empleado para obtener información de los bancos participantes. El cuestionario permite caracterizar ampliamente a los bancos y su gestión en Seginfo, de manera que se convierte en un activo muy valioso para la mejora continua de los bancos de la región. Con el fin de seguir mejorando, de permitir hacia el futuro un mejor uso de los datos por parte de la comunidad académica y enviar señales a los bancos sobre los temas que son importantes en gestión de Seginfo, el cuestionario debería ampliar las preguntas sobre gobernanza y tercerización de Seginfo, asegurando no solamente que se usen preguntas que permiten cuantificación matemática (p. ej., escalas Likert), sino que las preguntas recogen el conocimiento académico relevante sobre

estos temas, y debería incluir otros temas importantes, tales como las actitudes y cumplimiento de los empleados a la política de Seginfo, las actividades de creación y socialización de conocimiento en Seginfo, y más detalle sobre los esfuerzos en capacitación.

Finalmente, los mensajes para los bancos de la región son dos: la implementación de acciones y medidas técnicas (p. ej., comunicación cifrada, cortafuegos), sistemas de TI (p. ej., gestión de identidad, gestión de dispositivos móviles) y procesos (p. ej., evaluación de riesgos de terceros, monitoreo de amenazas) en materia de Seginfo está dando resultados para aumentar el nivel de detección interna de eventos adversos, y debe ser promovida. En cambio, la capacitación en Seginfo no está siendo efectiva en este mismo sentido, y debe fortalecerse para combatir preventivamente las racionalizaciones que impiden a los empleados cumplir con las políticas establecidas (ver Barlow *et al.*, 2018, para un ejemplo de cómo hacerlo), y también complementarse con un ecosistema de creación y socialización de conocimiento que les permita a los empleados participar más activamente y aprender unos de otros.

#### REFERENCIAS

- AJZEN, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)
- ALBUQUERQUE, A. E., & MARQUES DOS SANTOS, E. (2015). Adoption of information security measures in public research institutes. *Journal of Information Systems and Technology Management*, 12(2).
- ALKALBANI, A., DENG, H., KAM, B., & ZHANG, X. (2017). Information security compliance in organizations: An institutional perspective. *Data and Information Management*, 1(2), 104-114. <https://doi.org/10.1515/dim-2017-0006>
- ALMEIDA, L., & RESPÍCIO, A. (2018). Decision support for selecting information security controls. *Journal of Decision Systems*, 27(sup1), 173-180. <https://doi.org/10.1080/12460125.2018.1468177>
- AL-SAFWANI, N., FAZEA, Y., & IBRAHIM, H. (2018). ISCP: In-depth model for selecting critical security controls. *Computers & Security*, 77, 565-577. <https://doi.org/10.1016/j.cose.2018.05.009>

- ARHIN, K., & WIREDU, G. O. (2018). An organizational communication approach to information security. *The African Journal of Information Systems*, 10(4), 261-279.
- AURIGEMMA, S., & MATTSON, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information & Computer Security*, 25(4), 421-436. <https://doi.org/10.1108/ICS-11-2016-0089>
- BALOZIAN, P., LEIDNER, D., & WARKENTIN, M. (2019). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, 59(3), 197-210. <https://doi.org/10.1080/08874417.2017.1318687>
- BARLOW, J. B., WARKENTIN, M., ORMOND, D., & DENNIS, A. R. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, 19(8), 689-715. <https://doi.org/10.17705/1jais.00506>
- BAUER, S., & BERNROIDER, E. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: The Database for Advances in Information Systems*, 48(3), 44-68. <https://doi.org/10.1145/3130515.3130519>
- BAUER, S., BERNROIDER, E., & CHUDZIKOWSKI, K. (2013). End user information security awareness programs for improving information security in banking organizations: Preliminary results from an exploratory study. Ponencia presentada en Pre-ICIS Workshop on Information Security and Privacy (SIGSEC). <http://aisel.aisnet.org/wisp2012/33>
- BERKMAN, H., JONA, J., LEE, G., & SODERSTROM, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, 37(6), 508-526. <https://doi.org/10.1016/j.jaccpubpol.2018.10.003>
- BOSS, S. R., KIRSCH, L. J., ANGERMEIER, I., SHINGLER, R. A., & BOSS, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18, 151-164.
- BULGURCU, B., CAVUSOGLU, H., & BENBASAT, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.
- CAVUSOGLU, H., RAGHUNATHAN, S., & CAVUSOGLU, H. (2009). Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems. *Information Systems Research*, 20(2), 108-217. <https://doi.org/10.1287/isre.1080.0180>

- CEZAR, A., CAVUSOGLU, H., & RAGHUNATHAN, S. (2014). Outsourcing information security: Contracting issues and security implications. *Management Science*, 60(3), 638-657. <https://doi.org/10.1287/mnsc.2013.1763>
- CEZAR, A., CAVUSOGLU, H., & RAGHUNATHAN, S. (2017). Sourcing information security operations: The role of risk interdependency and competitive externality in outsourcing decisions. *Production and Operations Management*, 26(5), 860-879. <https://doi.org/10.1111/poms.12681>
- CHAI, S., KIM, M., & RAO, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, 50(4), 651-661. <https://doi.org/10.1016/j.dss.2010.08.017>
- CHANG, S. E., & HO, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), 345-361. <https://doi.org/10.1108/02635570610653498>
- CHEN, H., CHAU, P. Y. K., & LI, W. (2019). The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior. *Information Technology & People*, 32(4), 973-992. <https://doi.org/10.1108/ITP-12-2017-0421>
- CHEN, X., WU, D., CHEN, L., & TENG, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, 55(8), 1049-1060. <https://doi.org/10.1016/j.im.2018.05.011>
- CHMURA, J. (2017). Forming the awareness of employees in the field of information security. *Journal of Positive Management*, 8(1), 78-85. <https://doi.org/10.12775/JPM.2017.006>
- CHOI, M., & SONG, J. (2018). Social control through deterrence on the compliance with information security policy. *Soft Computing*, 22(20), 6765-6772. <https://doi.org/10.1007/s00500-018-3354-z>
- CHOI, S., MARTINS, J. T., & BERNIK, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science*, 44(6), 752-767. <https://doi.org/10.1177/0165551517748288>
- CRAM, W. A., D'ARCY, J., & PROUDFOOT, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2), 525-554. <https://doi.org/10.25300/MISQ/2019/15117>

- CROSSLER, R. E., JOHNSTON, A. C., LOWRY, P. B., HU, Q., WARKENTIN, M., & BASKERVILLE, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101. <https://doi.org/10.1016/j.cose.2012.09.010>
- CUGANESAN, S., STEELE, C., & HART, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology*, 37(1), 50-65. <https://doi.org/10.1080/0144929X.2017.1397193>
- D'ARCY, J., & TEH, P. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, 56(7), 103151. <https://doi.org/10.1016/j.im.2019.02.006>
- DANG-PHAM, D., PITTAYACHAWAN, S., & BRUNO, V. (2017a). Applying network analysis to investigate interpersonal influence of information security behaviours in the workplace. *Information & Management*, 54(5), 625-637. <https://doi.org/10.1016/j.im.2016.12.003>
- DANG-PHAM, D., PITTAYACHAWAN, S., & BRUNO, V. (2017b). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior*, 67, 196-206. <https://doi.org/10.1016/j.chb.2016.10.025>
- DOHERTY, N. F., & FULFORD, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal*, 18(4), 21-39. <https://doi.org/10.4018/irmj.2005100102>
- DOHERTY, N. F., & TAJUDDIN, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. *Information Technology & People*, 31(2), 348-367. <https://doi.org/10.1108/ITP-08-2016-0194>
- FISHBEIN, M. (1967). A behavior theory approach to the relations between beliefs about an object and the attitude toward the object. En M. Fishbein (ed.), *Readings in attitude theory and measurement* (pp. 389-400). John Wiley & Sons.
- FRISKEN, J. (2015). Leveraging COBIT to implement information security. *COBIT Focus*, 1-7. <https://doi.org/10.4018/978-1-59904-924-3.ch002>
- GAL-OR, E., & GHOSE, A. (2005). The economic incentives for sharing security information. *Information Systems Research*, 16(2), 186-208. <https://doi.org/10.1287/isre.1050.0053>

- GORDON, L. A., & LOEB, M. P. (2006). Budgeting process for information security expenditures. *Communications of the ACM*, 49, 121-125. <https://doi.org/10.1145/1107458.1107465>
- GORDON, L. A., LOEB, M. P., & ZHOU, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1), 33-56. <https://doi.org/10.3233/JCS-2009-0398>
- GORDON, W. J., WRIGHT, A., GLYNN, R. J., KADAKIA, J., MAZZONE, C., LEINBACH, E., & LANDMAN, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association: JAMIA*, 26(6), 547-552. <https://doi.org/10.1093/jamia/ocz005>
- HADLINGTON, L., & PARSONS, K. (2017). Can cyberloafing and internet addiction affect organizational information security? *Cyberpsychology, Behavior, and Social Networking*, 20(9), 567-571. <https://doi.org/10.1089/cyber.2017.0239>
- HAN, J., KIM, Y. J., & KIM, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security*, 66, 52-65. <https://doi.org/10.1016/j.cose.2016.12.016>
- HAUFE, K., COLOMO-PALACIOS, R., DZOMBETA, S., BRANDIS, K., & STANTCHEV, V. (2016). Security management standards: A mapping. *Procedia Computer Science*, 100, 755-761. <https://doi.org/10.1016/j.procs.2016.09.221>
- HE, Y., & JOHNSON, C. (2017). Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. *Informatics for Health and Social Care*, 42(4), 393-408. <https://doi.org/10.1080/17538157.2016.1255629>
- HERATH, T., & RAO, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165. <https://doi.org/10.1016/j.dss.2009.02.005>
- HERATH, T., YIM, M., D'ARCY, J., NAM, K., & RAO, H. R. (2018). Examining employee security violations: Moral disengagement and its environmental influences. *Information Technology & People*, 31(6), 1135-1162. <https://doi.org/10.1108/ITP-10-2017-0322>
- HINZ, O., NOFER, M., SCHIERECK, D., & TRILLIG, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, 52(3), 337-347. <https://doi.org/10.1016/j.im.2014.12.006>

- HOHAN, A. I., OLARU, M., & PIRNEA, I. C. (2015). Assessment and continuous improvement of information security based on TQM and business excellence principles. *Procedia Economics and Finance*, 32, 352-359. [https://doi.org/10.1016/S2212-5671\(15\)01404-5](https://doi.org/10.1016/S2212-5671(15)01404-5)
- Hou, Y., GAO, P., & NICHOLSON, B. (2018). Understanding organisational responses to regulative pressures in information security management: The case of a Chinese hospital. *Technological Forecasting & Social Change*, 126, 64-75. <https://doi.org/10.1016/j.techfore.2017.03.023>
- HU, Q., DINEV, T., HART, P., & COOKE, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-660. <https://doi.org/10.1111/j.1540-5915.2012.00361.x>
- HU, Q., WEST, R., & SMARANDESCU, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, 31(4), 6-48. <https://doi.org/10.1080/07421222.2014.1001255>
- HUI, K., HUI, W., & YUE, W. T. (2012). Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems*, 29(3), 117-156. <https://doi.org/10.2753/MIS0742-1222290304>
- HUMAYDI, N., & BALAKRISHNAN, V. (2018). Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Information Management Journal*, 47(1), 17-27.
- HWANG, I., & CHA, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, 81, 282-293. <https://doi.org/10.1016/j.chb.2017.12.022>
- IFINEDO, P. (2016). Critical times for organizations: What should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management*, 33(1), 30-41. <https://doi.org/10.1080/10580530.2015.1117868>
- JEONG, C. Y., LEE, S. T., & LIM, J. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, 56, 681-695. <https://doi.org/10.1016/j.im.2018.11.003>
- JOHNSTON, A. C., DI GANGI, P. M., HOWARD, J., & WORRELL, J. (2019). It takes a village: Understanding the collective security efficacy of employee groups.

- Journal of the Association for Information Systems*, 20(3), 186-212. <https://doi.org/10.17705/1jais.00533>
- KAJTAZI, M., CAVUSOGLU, H., BENBASAT, I., & HAFTOR, D. (2018). Escalation of commitment as an antecedent to noncompliance with information security policy. *Information & Computer Security*, 26(2), 171-193. <https://doi.org/10.1108/ICS-09-2017-0066>
- KANKANHALLI, A., TEO, H., TAN, B. C. Y., & WEI, K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23, 139-154.
- KARANJA, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security*, 25(3), 300-329. <https://doi.org/10.1108/ICS-02-2016-0013>
- KARANJA, E., & ROSSO, M. A. (2017). The chief information security officer: An exploratory study. *Journal of International Technology and Information Management*, 26(2), 23-47.
- KARLSSON, F., KARLSSON, M., & ÅSTRÖM, J. (2017). Measuring employees' compliance – the importance of value pluralism. *Information & Computer Security*, 25(3), 279-299. <https://doi.org/10.1108/ICS-11-2016-0084>
- KARLSSON, M., DENK, T., & ÅSTRÖM, J. (2018). Perceptions of organizational culture and value conflicts in information security management. *Information & Computer Security*, 26(2), 213-229. <https://doi.org/10.1108/ICS-08-2017-0058>
- KERTI, A., & NYIKES, Z. (2015). Overview of the information security standardization. *Acta Technica Corviniensis - Bulletin of Engineering*, 8(3), 109.
- KIM, H. L., & HAN, J. (2019). Do employees in a “good” company comply better with information security policy? A corporate social responsibility perspective. *Information Technology & People*, 32(4), 858-875. <https://doi.org/10.1108/ITP-09-2017-0298>
- KNAPP, K. J., MARSHALL, T. E., RAINER, R. K., & FORD, F. N. (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24-36. <https://doi.org/10.1108/09685220610648355>
- KORTE, J. (2017). Mitigating cyber risks through information sharing. *Journal of Payments Strategy & Systems*, 11(3), 203-214.

- KWON, J., & JOHNSON, M. E. (2018). Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quarterly*, 42(4), 1043-1067. <https://doi.org/10.25300/MISQ/2018/13580>
- KWON, J., ULMER, J. R., & WANG, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, 27(1), 219-236. <https://doi.org/10.2308/isys-50339>
- LAYTON, T. P. (2007). *Information security: Design, implementation, measurement and compliance*. Auerbach Publications.
- LEE, C., LEE, C. C., & KIM, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, 59, 60-70. <https://doi.org/10.1016/j.cose.2016.02.004>
- LOWRY, P. B., & MOODY, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, 25(5), 433-463. <https://doi.org/10.1111/isj.12043>
- LOWRY, P. B., POSEY, C., BENNETT, R. J., & ROBERTS, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, 25(3), 193-230. <https://doi.org/10.1111/isj.12063>
- MA, Q., & PEARSON, J. M. (2005). ISO 17799: "Best practices" in information security management? *Communications of the Association for Information Systems*, 15, 577-591. <https://doi.org/10.17705/ICAIS.01532>
- MCLAUGHLIN, M., & GOGAN, J. (2018). Challenges and best practices in information security management. *MIS Quarterly Executive*, 17(3), 237-262.
- MENARD, P., BOTT, G. J., & CROSSLER, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, 34(4), 1203-1230. <https://doi.org/10.1080/07421222.2017.1394083>
- MEOLA, A. (2019, 8 de agosto). The digital trends disrupting the banking industry in 2020. *Business Insider*. <https://www.businessinsider.com/banking-industry-trends>

- MIJNHARDT, F., BAARS, T., & SPRUIT, M. (2016). Organizational characteristics influencing SME information security maturity. *The Journal of Computer Information Systems*, 56(2), 106-115.
- NAICKER, V., & MAFAITI, M. (2019). The establishment of collaboration in managing information security through multisourcing. *Computers & Security*, 80, 224-237. <https://doi.org/10.1016/j.cose.2018.10.005>
- NEL, F., & DREVIN, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security*, 27(2), 146-164. <https://doi.org/10.1108/ICS-12-2016-0095>
- NICHO, M. (2018). A process model for implementing information systems security governance. *Information & Computer Security*, 26(1), 10-38. <https://doi.org/10.1108/ICS-07-2016-0061>
- NJENGA, K., & JORDAAN, P. (2016). We want to do it our way: The neutralization approach to managing information systems security by small businesses. *The African Journal of Information Systems*, 8(1), 42-63.
- OEA. (2018). *Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe*. Organización de Estados Americanos. <https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp>
- OSMANBEGOVI, E., PIRI, N., & SULJI, M. (2017). Information security controls as determinant of continuity of information system work. *Economic Review - Journal of Economics and Business*, 15(2), 35-42.
- PAANANEN, H., LAPKE, M., & SIPONEN, M. (2020). State of the art in information security policy development. *Computers & Security*, 88, 101608. <https://doi.org/10.1016/j.cose.2019.101608>
- PAHNILA, S., SIPONEN, M., & MAHMOOD, A. (2007). Employees' behavior towards IS security policy compliance. *40th Hawaii International Conference on System Sciences* (p. 156b). Hawaii: IEEE. <https://doi.org/10.1109/HICSS.2007.206>
- PÉREZ-GONZÁLEZ, D., TRIGUEROS PRECIADO, S., & SOLANA-GONZÁLEZ, P. (2019). Organizational practices as antecedents of the information security management performance. *Information Technology & People*, 32(5), 1262-1275. <https://doi.org/10.1108/ITP-06-2018-0261>
- PHAM, H. C., BRENNAN, L., & FURNELL, S. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and

- resources. *Journal of Information Security and Applications*, 46, 96-107. <https://doi.org/10.1016/j.jisa.2019.03.012>
- RAHMAN, N. H. A., & CHOO, R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, 49, 45-69.
- ROCHA FLORES, W., & EKSTEDT, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, 59, 26-44.
- SAINT-GERMAIN, R. (2005). Information security management best practice based on ISO/IEC 17799. *The Information Management Journal*, July/August, 60.
- SCHATZ, D., & BASHROUSH, R. (2016). The impact of repeated data breach events on organisations' market value. *Information & Computer Security*, 24(1), 73-92. <https://doi.org/10.1108/ICS-03-2014-0020>
- SILVA, L., HSU, C., BACKHOUSE, J., & McDONNELL, A. (2016). Resistance and power in a security certification scheme: The case of c:Cure. *Decision Support Systems*, 92, 68-78. <https://doi.org/10.1016/j.dss.2016.09.014>
- SIPONEN, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41. <https://doi.org/10.1108/09685220010371394>
- SIPONEN, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, 49, 97-100. <https://doi.org/10.1145/1145287.1145316>
- SIPONEN, M., MAHMOOD, M. A., & PAHNILA, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217-224. <https://doi.org/10.1016/j.im.2013.08.006>
- SIPONEN, M., & VANCE, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-502. <https://doi.org/10.2307/25750688>
- SIPONEN, M., & WILLISON, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, 46(5), 267-270. <https://doi.org/10.1016/j.im.2008.12.007>

- SOMMESTAD, T. (2018). Work-related groups and information security policy compliance. *Information & Computer Security*, 26(5), 533-550. <https://doi.org/10.1108/ICS-08-2017-0054>
- SOMMESTAD, T., HALLBERG, J., LUNDHOLM, K., & BENGTTSSON, J. (2014). Variables influencing information security policy compliance. *Information Management & Computer Security*, 22(1), 42-75. <https://doi.org/10.1108/IMCS-08-2012-0045>
- SOOMRO, Z. A., SHAH, M. H., & AHMED, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225. <https://doi.org/10.1016/j.ijinfomgt.2015.11.009>
- SPANOS, G., & ANGELIS, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, 58, 216-229. <https://doi.org/10.1016/j.cose.2015.12.006>
- SUSANTO, H., ALMUNAWAR, M. N., & TUAN, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences*, 11, 23-29. <https://doi.org/10.1007/S11623-011-0004-3>
- Technisys. (2016). *Digital banking in Latin America: Trends, challenges and priorities in today's scenario*. [https://www.technisys.com/wp-content/uploads/2017/02/Digital-Banking-in-Latin-America\\_EN.pdf](https://www.technisys.com/wp-content/uploads/2017/02/Digital-Banking-in-Latin-America_EN.pdf)
- TSOHOU, A., KARYDA, M., & KOKOLAKIS, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, 52, 128-141. <https://doi.org/10.1016/j.cose.2015.04.006>
- TU, C. Z., YUAN, Y., ARCHER, N., & CONNELLY, C. E. (2018). Strategic value alignment for information security management: A critical success factor analysis. *Information & Computer Security*, 26(2), 150-170. <https://doi.org/10.1108/ICS-06-2017-0042>
- ULA, M., ISMAIL, Z., & SIDEK, Z. (2011). A framework for the governance of information security in banking system. *Journal of Information Assurance & Cybersecurity*, 2011, 1-12. <https://doi.org/10.5171/2011.726196>
- WANG, J., SHAN, Z., GUPTA, M., & RAO, H. R. (2019). A longitudinal study of unauthorized access attempts on information systems: The role of opportunity contexts. *MIS Quarterly*, 43(2), 601-622. <https://doi.org/10.25300/MISQ/2019/14751>

- WEST, R., BUDDE, E., & HU, Q. (2019). Neural correlates of decision making related to information security: Self-control and moral potency. *PLoS One*, 14(9), 1-21. <https://doi.org/10.1371/journal.pone.0221808>
- WHITMAN, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, 24(1), 43-57. <https://doi.org/10.1016/j.ijinfomgt.2003.12.003>
- WU, Y., FENG, G., WANG, N., & LIANG, H. (2015). Game of information security investment: Impact of attack types and network vulnerability. *Expert Systems with Applications*, 42(15-16), 6132-6146. <https://doi.org/10.1016/j.eswa.2015.03.033>
- YAYLA, A. A., & HU, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, 26(1), 60-77. <https://doi.org/10.1057/jit.2010.4>
- YAZDANMEHR, A., & WANG, J. (2016). Employees' information security policy compliance: A norm activation perspective. *Decision Support Systems*, 92, 36-46. <https://doi.org/10.1016/j.dss.2016.09.009>
- ZAFAR, H., KO, M. S., & OSEI-BRYSON, K. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers*, 18(6), 1205-1215. <https://doi.org/10.1007/s10796-015-9562-5>
- ZHANG, H., CHARL, K., & AGRAWAL, M. (2018). Decision support for the optimal allocation of security controls. *Decision Support Systems*, 115, 92-104. <https://doi.org/10.1016/j.dss.2018.10.001>
- ZHANG, X., WUWONG, N., LI, H., & ZHANG, X. (2010). Information security risk management framework for the cloud computing environments. *10th IEEE International Conference on Computer and Information Technology (CIT 2010)* (pp. 1328-1334). Bradford, UK. [HTTPS://DOI.ORG/10.1109/CIT.2010.501](https://doi.org/10.1109/CIT.2010.501)
- ZHAO, L., MEI, S., & ZHONG, W. (2015). An economic analysis of the interactions between firewall, IDS and vulnerability scan. *Economic Computation and Economic Cybernetics Studies and Research*, (4), 323-340.

ANEXO I: CONVERSIÓN DE LAS RESPUESTAS DEL CUESTIONARIO ORIGINAL DE LA OEA A ESCALAS NUMÉRICAS

Nombre del constructo	N.º ítem	Pregunta cuestionario OEA	Medición original OEA (opciones de respuesta)	Conversión para este estudio
Modelo de gobierno y apoyo de la alta gerencia	1	Entendiendo que el CEO del banco al cual usted pertenece es la cabeza de la institución (nivel 0), ¿cuántos niveles jerárquicos hay entre el CEO y el máximo responsable de la seguridad digital?	- Más de tres (3) niveles - Tres (3) niveles - Dos (2) niveles - Un (1) nivel	Más de tres (3) niveles: 1 Tres (3) niveles: 2 Dos (2) niveles: 3 Un (1) nivel: 4
	2	Como parte del modelo de gobierno de la institución, ¿la junta directiva del banco al cual usted pertenece recibe reportes periódicos acerca de indicadores y gestión de riesgos de seguridad digital?	- No - Sí	No: 1 Sí: 2
	3	¿Cómo demuestra la alta dirección del banco al cual usted pertenece el apoyo a la gestión del riesgo de seguridad digital? Múltiples respuestas pueden ser posibles.	Siete alternativas de respuesta tipo texto. Ejemplos: exigiendo la adopción de buenas prácticas de seguridad, impulsando planes de seguridad digital, etc.	Escala de 1 a 7. Cada respuesta marcada equivale a una unidad, y las unidades se acumulan hasta un máximo de 7.
	4	¿Cuán complejo es, en su opinión, convencer a la alta dirección del banco al cual usted pertenece de invertir en soluciones de seguridad digital?	- Muy complejo - Medianamente complejo - Poco complejo	Muy complejo: 1 Medianamente complejo: 2 Poco complejo: 3
	5	¿Cuál fue el presupuesto de seguridad digital del banco al cual usted pertenece para el actual año fiscal?	- No tiene presupuesto asignado - Menos del 1 % del Ebitda del año anterior - Entre 1 % y 5 % del Ebitda del año anterior - Más del 5 % del Ebitda del año anterior	No tiene presupuesto asignado: 1 Menos del 1 % del Ebitda: 2 Entre 1 % y 5 % del Ebitda: 3 Más del 5 % del Ebitda: 4

Nombre del constructo	N.º ítem	Pregunta cuestionario OEA	Medición original OEA (opciones de respuesta)	Conversión para este estudio
Buenas prácticas de gestión de TI/ Seginfo	1	¿Cuáles servicios externos ( <i>outsourcing</i> ) tiene contratado el banco al cual usted pertenece para adelantar las siguientes actividades relacionadas con la seguridad digital? Múltiples respuestas pueden ser posibles.	Doce alternativas de respuesta tipo texto. Ejemplos: pruebas de seguridad, monitoreo de controles de seguridad, etc.	Escala de 1 a 12. Cada respuesta marcada equivale a una unidad, y las unidades se acumulan hasta un máximo de 12.
	2	¿El banco al cual usted pertenece ha adoptado los siguientes marcos de seguridad y/o estándares internacionales? Múltiples respuestas pueden ser posibles.	Diez alternativas de respuesta tipo texto. Ejemplos: ISO 27000, Cobit, etc.	Escala de 1 a 10. Cada respuesta marcada equivale a una unidad, y las unidades se acumulan hasta un máximo de 10.
	3	¿Qué tipo de acciones y medidas técnicas de seguridad digital tiene el banco al cual usted pertenece para proteger los sistemas de información críticos? Múltiples respuestas pueden ser posibles.	Nueve alternativas de respuesta tipo texto. Ejemplos: comunicación cifrada, cortafuegos, etc.	Escala de 1 a 9. Cada respuesta marcada equivale a una unidad, y las unidades se acumulan hasta un máximo de 9.
	4	¿Qué tipo de sistemas de seguridad digital tiene el banco al cual usted pertenece para proteger los sistemas de información críticos? Múltiples respuestas pueden ser posibles.	Siete alternativas de respuesta tipo texto. Ejemplos: gestión de identidad, gestión de dispositivos móviles, etc.	Escala de 1 a 7. Cada respuesta marcada equivale a una unidad, y las unidades se acumulan hasta un máximo de 7.
	5	¿Qué tipo de procesos de seguridad digital tiene el banco al cual usted pertenece para proteger los sistemas de información críticos? Múltiples respuestas pueden ser posibles.	Ocho alternativas de respuesta tipo texto. Ejemplos: evaluación de riesgos de terceros, monitoreo de amenazas, etc.	Escala de 1 a 8. Cada respuesta marcada equivale a una unidad, y las unidades se acumulan hasta un máximo de 8.

Nombre del cons-tructo	N.º ítem	Pregunta cuestionario OEA	Medición original OEA (opciones de respuesta)	Conversión para este estudio
	6	¿El banco al cual usted pertenece cuenta y ejecuta las siguientes estrategias frente a incidentes (ataques exitosos) de seguridad digital?	<ul style="list-style-type: none"> <li>- Priorización - No</li> <li>- Priorización - Sí</li> <li>- Contención - No</li> <li>- Contención - Sí</li> <li>- Respuesta - No</li> <li>- Respuesta - Sí</li> <li>- Recuperación - No</li> <li>- Recuperación - Sí</li> </ul>	<p>Cada No: 1 Cada Sí: 2 Se suman todas las respues-tas.</p>
Buenas prácticas de gestión de TI/ Seginfo	7	¿El banco al cual usted pertenece ha sido valorado externamente en los últimos dos (2) años mediante alguna metodología de evaluación de la madurez de seguridad digital y ha completado dicha evaluación?	<ul style="list-style-type: none"> <li>- No, nuestro banco no ha sido valo-rado</li> <li>- Sí se realizó la evaluación, pero no ha sido posible adelantar las acciones correspondientes</li> <li>- Sí se realizó la evaluación y se están adelantando actualmente las acciones correspondientes</li> <li>- Sí se realizó la evaluación y se ejecu-taron satisfactoriamente las acciones correspondientes</li> </ul>	<p>No: 1 Sí se realizó la evaluación, pero...: 2 Sí se realizó la evaluación y se están...: 3 Sí se realizó la evaluación y se ejecutaron...: 4</p>
	8	¿El banco al cual usted pertenece cuenta con un plan de comunicaciones que permita informar a sus clientes de servicios financieros cuando su información personal se haya visto comprometida?	<ul style="list-style-type: none"> <li>- No</li> <li>- Sí</li> </ul>	<p>No: 1 Sí: 2</p>

Nombre del constructo	N.º ítem	Pregunta cuestionario OEA	Medición original OEA (opciones de respuesta)	Conversión para este estudio
Gestión personal en Seginfo	1	a- ¿Cuántas personas conforman la totalidad de equipos que manejan procesos asociados a la seguridad digital en el banco al cual usted pertenece, sin incluir personal de empresas que prestan servicios externos ( <i>outsourcing</i> )?	<ul style="list-style-type: none"> <li>- Entre 1 y 5</li> <li>- Entre 6 y 15</li> <li>- Entre 16 y 30</li> <li>- Entre 31 y 60</li> <li>- Entre 61 y 120</li> <li>- Entre 121 y 300</li> <li>- 301 o más</li> </ul>	Razón entre a y b, construida así: Límite inferior respuesta pregunta a / Límite inferior respuesta pregunta b
		b- ¿Cuántos empleados tiene el banco al cual usted pertenece?	<ul style="list-style-type: none"> <li>- Hasta 300</li> <li>- Entre 301 y 999</li> <li>- Entre 1.000 y 4.999</li> <li>- 5.000 o más</li> </ul>	Ej.: a - Entre 61 y 120 b - Entre 1.000 y 4.999 Entonces: 61/1.000 = 0.061
	2	¿El banco al cual usted pertenece ofrece un mecanismo para que sus usuarios internos (empleados y contratistas) reporten incidentes (ataques exitosos) de seguridad digital sufridos?	<ul style="list-style-type: none"> <li>- No</li> <li>- Sí</li> </ul>	No: 1 Sí: 2
	3	a- ¿Cuenta el banco al cual usted pertenece con planes de preparación, respuesta y capacitación en asuntos de seguridad digital para sus empleados e <i>insourcing</i> bancarios? b- ¿Con qué frecuencia se ejecutan dichos planes de preparación, respuesta y capacitación?	<ul style="list-style-type: none"> <li>- No</li> <li>- Sí</li> <li>- Anual</li> <li>- Semestral</li> <li>- Trimestral</li> </ul>	No: 1 Anual: 2 Semestral: 3 Trimestral: 4
	4	¿Con qué frecuencia se prueba la capacidad de los empleados del banco al cual usted pertenece para responder adecuadamente frente a incidentes (ataques exitosos) de seguridad digital y esquemas de <i>phishing</i> e ingeniería social?	<ul style="list-style-type: none"> <li>- Nunca</li> <li>- Anual</li> <li>- Semestral</li> <li>- Trimestral</li> </ul>	Nunca: 1 Anual: 2 Semestral: 3 Trimestral: 4

Nombre del cons-tructo	N.º ítem	Pregunta cuestionario OEA	Medición original OEA (opciones de respuesta)	Conversión para este estudio
Detección interna de eventos	1	<p>¿Qué porcentaje de eventos de seguridad digital son detectados mediante sistemas propios (y no de terceros) de detección del banco al cual usted pertenece?</p>	<ul style="list-style-type: none"> <li>- Del 0 % al 20 %</li> <li>- Del 21 % al 40 %</li> <li>- Del 41 % al 60 %</li> <li>- Del 61 % al 80 %</li> <li>- Del 81 % al 100 %</li> </ul>	<ul style="list-style-type: none"> <li>Del 0 % al 20 %: 1</li> <li>Del 21 % al 40 %: 2</li> <li>Del 41 % al 60 %: 3</li> <li>Del 61 % al 80 %: 4</li> <li>Del 81 % al 100 %: 5</li> </ul>
Ocurren-cia de eventos	1 ... 14	<p>¿Qué tipos de eventos de seguridad digital contra el banco al cual usted pertenece se han identificado durante los últimos doce meses? Para cada tipo, por favor indique la frecuencia aproximada de ocurrencia. Los catorce tipos de eventos son:</p> <ul style="list-style-type: none"> <li>- Ingeniería social</li> <li>- Código malicioso o <i>malware</i></li> <li>- <i>Phishing</i> dirigido para tener acceso a sistemas del banco</li> <li>- Pérdida de datos</li> <li>- Pérdida o robo de equipos o dispositivos</li> <li>- Ataque de negación del servicio (DoS / DDoS)</li> <li>- Robo de DNS</li> <li>- Violación de políticas de escritorio limpio (<i>clear desk</i>)</li> <li>- Sabotaje interno</li> <li>- Fraude interno</li> <li>- Defacement</li> <li>- Backdoor (código para habilitar acceso posterior)</li> <li>- SQL Injection</li> <li>- Ataque de fuerza bruta</li> </ul>	<ul style="list-style-type: none"> <li>- No hay</li> <li>- Trimestral</li> <li>- Mensual</li> <li>- Semanal</li> <li>- Diario</li> </ul>	<ul style="list-style-type: none"> <li>No hay: 5</li> <li>Trimestral: 4</li> <li>Mensual: 3</li> <li>Semanal: 2</li> <li>Diario: 1</li> </ul>

Nombre del constructo	N.º ítem	Pregunta cuestionario OEA	Medición original OEA (opciones de respuesta)	Conversión para este estudio
Impacto económico	1	<p>a- ¿El banco al cual usted pertenece ha llevado a cabo cálculos de retorno sobre la inversión en seguridad digital?</p> <p>b- ¿Cuál fue el retorno sobre la inversión en seguridad digital para su banco en el año fiscal inmediatamente anterior? Por favor exprese su respuesta como un número entero equivalente a un porcentaje (por ejemplo; 30 indica 30 %).</p>	<p>- No</p> <p>- Sí</p> <p>o a 100</p>	<p>Se retuvieron las respuestas que dijeron "Sí" en la pregunta a.</p> <p>o a 100</p>
	2	<p>a- ¿El banco al cual usted pertenece estimó el costo total de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad digital para el último año fiscal?</p> <p>b- ¿Cuál fue el costo de respuesta y de recuperación ante incidentes (ataques exitosos) en seguridad digital para el banco al cual usted pertenece para el último año fiscal?</p>	<p>- No</p> <p>- Sí</p> <p>- Entre 1 % y 5 % del Ebitda del año anterior</p> <p>- Menos del 1 % del Ebitda del año anterior</p>	<p>Se retuvieron las respuestas que dijeron "Sí" en la pregunta a.</p> <p>- Entre 1 % y 5 % del Ebitda: 1</p> <p>- Menos del 1 % del Ebitda: 2</p>
Grado de penetración de operaciones no presenciales	1	<p>Del total de operaciones del banco al cual usted pertenece, qué porcentaje se realizó por medio de canales transaccionales no presenciales (internet, transacciones electrónicas, cajeros automáticos, pagos automáticos, telefonía móvil y audio-respuesta) durante los últimos doce meses:</p>	<p>- Del 0 % al 20 %</p> <p>- Del 21 % al 40 %</p> <p>- Del 41 % al 60 %</p> <p>- Del 61 % al 80 %</p> <p>- Del 81 % al 100 %</p>	<p>Del 0 % al 20 %: 1</p> <p>Del 21 % al 40 %: 2</p> <p>Del 41 % al 60 %: 3</p> <p>Del 61 % al 80 %: 4</p> <p>Del 81 % al 100 %: 5</p>

La tercera edición de la colección “Así habla el Externado” examina el impacto que las tecnologías disruptivas y la transformación digital están teniendo sobre el conjunto de la sociedad, bajo una lente humanista e interdisciplinar, propia de nuestra institución. La Cuarta Revolución Industrial (4RI), que ha permeado todos los campos de la actividad humana y la sociedad, ofrece la inmensa oportunidad de reducir las brechas de conocimiento e ingreso económico y generar progreso social y democrático, pero puede también tener el efecto contrario. El lector y la lectora encontrarán en estos cuatro tomos reflexiones valiosas, en sus 74 escritos, para comprender en todo su alcance estas innovaciones y poder contribuir así a la construcción de realidades cada vez más incluyentes y participativas.

\* \* \* \* \*

Este tomo constituye una invitación a reflexionar sobre el hecho de que las nuevas tecnologías digitales, particularmente aquellas asociadas a la 4RI, tales como la inteligencia artificial y el *Blockchain*, representan un gran desafío para las instituciones sociales que típicamente entendemos como dadas y estables, tales como el sistema capitalista, las monedas nacionales o el trabajo remunerado. Recordemos que las grandes instituciones sociales no son cuestionadas a diario, puesto que su permanencia en el tiempo es un factor esencial de continuidad y estabilidad de los procesos sociales. Por esta razón, las transformaciones institucionales relacionadas con la 4RI demandan no solo un estudio atento, sino una mirada humanista, plural y propositiva en procura de resultados deseables para todos los actores inmersos en estos cambios. Los trabajos aquí contenidos apuntan en esa dirección.

