Capítulo 5

Guía para la adopción de una cultura de ciberseguridad en juntas directivas*

DOI: https://doi.org/10.25062/9786287818002.05

Milena Carvajal Bernal
Caja de Compensación Familiar Compensar

Resumen: Esta investigación propone un instrumento práctico para que las juntas directivas adopten una cultura de ciberseguridad, considerando elementos como la generación de conciencia entre sus integrantes y la gestión temprana de los riesgos que puedan impactar negativamente en la organización. Asimismo, se establece la innovación tecnológica como un factor relevante para la colaboración organizacional. Se reconoce al ser humano como un elemento clave en la solución de los desafíos en seguridad de la información y ciberseguridad, cuyo comportamiento y adopción de estrategias basadas en tecnología contribuyen a mejorar el entorno empresarial en esta materia. Se desarrolla bajo un enfoque cualitativo, basado en los resultados de encuestas y en el análisis de la información recopilada durante su ejecución. Como resultado y conclusión, se presenta una guía con elementos, pasos y recomendaciones para adoptar una cultura de ciberseguridad en las juntas directivas.

Palabras clave: ciberseguridad; cultura organizacional; gestión empresarial; innovación; tecnología.

* Capítulo de libro resultado del proyecto de investigación *"Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales"* del grupo de investigación "Ciberespacio Tecnología e Innovación", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado C por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0181179. Los puntos de vista y los resultados de este capítulo pertenecen al autor y no reflejan necesariamente los de las instituciones participantes.

Milena Carvajal Bernal
Magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Especialista en Gerencia de Proyectos de Sistemas, Universidad del Rosario, Colombia. Ingeniera de sistemas, Universidad Manuela Beltrán, Colombia.
https://orcid.org/0009-0006-9721-8541 - Contacto: **carvajalmi@esdeg.edu.co**

Citación APA: Carvajal Bernal, M. (2025). Guía para la adopción de una cultura de ciberseguridad en juntas directivas. En M. E. Realpe Díaz & G. A. Gómez Rodríguez (Eds.), *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales* (pp. 157-196). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818002.05

CIBERSEGURIDAD EN LA FRONTERA DIGITAL: DESAFÍOS Y OPORTUNIDADES EN LOS NUEVOS ECOSISTEMAS TECNOLÓGICOS EMPRESARIALES
ISBN impreso: 978-628-7602-99-1
ISBN digital: 978-628-7818-00-2
DOI: https://doi.org/10.25062/9786287818002

Colección Ciberseguridad y Ciberdefensa
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Introducción

La ciberseguridad debe considerarse un elemento esencial en las organizaciones. Su importancia en el contexto de la transformación digital requiere el respaldo de los niveles directivos para fomentar una cultura preventiva frente a escenarios de riesgo.

En Colombia, la promoción de una cultura de ciberseguridad ha sido objeto de discusión desde hace años. Documentos como el CONPES 3701 (2011) y la resolución AG/RES. 2004 (34-O/04) de la Organización de Estados Americanos (OEA, 2004) ofrecen lineamientos para la implementación de una cultura de ciberseguridad a nivel nacional y regional, respectivamente.

Por otro lado, en la era digital, la cultura y la tecnología están estrechamente relacionadas. La tecnología influye en el comportamiento de una sociedad al cambiar las prácticas culturales, y, a su vez, la dirección en la que avanza la tecnología está ligada estrictamente a lo que determine una sociedad (Goicoechea, 2004). Esta relación puede entenderse a través del principio de equifinalidad de la teoría general de sistemas (TGS), que sugiere que sistemas abiertos como la tecnología pueden alcanzar los mismos objetivos finales a partir de diferentes condiciones iniciales (Bertalanffy, 1989).

Un aspecto relevante en el campo de la tecnología es la cuarta revolución industrial, la cual se desarrolla a un ritmo acelerado, trayendo consigo desafíos significativos en términos de ciberseguridad, como la hiperconectividad de sistemas que genera brechas de seguridad considerables que deben ser abordadas desde todos los puntos de vista posibles. Por tanto, la concientización y comprensión de los riesgos latentes por parte de todos los sectores permitirá crear estructuras más conscientes que fomenten la colaboración entre las personas y las organizaciones, asumiendo una responsabilidad de prevención durante la cuarta revolución industrial (Schwab, 2016).

Sin embargo, una percepción común es que, cuando se habla de ciberseguridad, la mayor parte de las veces se cree que esta es una responsabilidad del equipo de tecnologías de la información (TI) y que no trasciende más allá de las fronteras tecnológicas, cuando, por el contrario, es un tema que debe ser responsabilidad de toda la organización, comenzando por las juntas directivas, quienes "no están tan involucradas en la ciberseguridad como lo están en otras áreas de supervisión" (Gale et al., 2022; Willie, 2023).

Esta mentalidad podría llevar a eventos con impactos negativos para las compañías y, a su vez, para las personas que conforman las juntas directivas. Estas últimas son quienes eventualmente deberán responder legalmente ante cualquier desviación o incumplimiento que se genere por su desconocimiento u omisión. Por lo tanto, para que haya un compromiso de los directores con la ciberseguridad, se requiere en muchos casos que exista una regulación, la cual es denominada por Gale et al. (2022) como "fuerza coercitiva", que les obligue al cumplimiento de una ley para implementar medidas de ciberseguridad para la protección de la confidencialidad, integridad y disponibilidad de la información.

Tomando el ejemplo que relata Jen Pascua, director de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA, por sus siglas en inglés), en el "Manual del director sobre supervisión de riesgos cibernéticos", se plantea el caso de un CISO que propone implementar un sistema de doble factor de autenticación (MFA) para mitigar los riesgos de *phishing* en la compañía. Ante esto, los directores se niegan argumentando que el costo de implementación es muy alto en comparación con la probabilidad de un ataque cibernético, resultando en un ataque real con consecuencias negativas para la empresa (Clinton et al., 2023). Este es un claro ejemplo de cómo la responsabilidad de las juntas directivas es crucial en el contexto actual, en el que hay una gran brecha de conocimientos en cuanto a ciberseguridad y la adopción de una cultura organizacional al respecto.

Según el informe de IBM para el primer trimestre de 2023, los riesgos están aumentando exponencialmente, identificando que los vectores de ataque que más pérdidas generan incluyen atacantes internos, *phishing* y el compromiso de cuentas de correo dirigidas a los directivos (BEC, por sus siglas en inglés) (IBM Security, 2023). Esto evidencia que el ser humano y sus comportamientos son elementos que pueden poner en riesgo la seguridad empresarial, basado en sus prácticas (Cano, 2021), y, por lo tanto, deben contemplarse como parte integral de una estrategia de ciberseguridad corporativa (Willie, 2023).

El informe del Instituto de Auditores Internos (IIA, 2021) indica que, aunque los miembros directivos son conscientes de los riesgos de ciberseguridad, a menudo carecen del conocimiento y la preparación adecuados para abordarlos de manera efectiva. Esta falta de preparación se debe, en parte, a que la ciberseguridad aún se considera como "un problema principalmente técnico" (Gale et al., 2022, p. 4).

Para lograr un compromiso efectivo de la alta dirección en materia de ciberseguridad, resulta fundamental asignar recursos humanos y de infraestructura. No obstante, esto no es suficiente; las organizaciones también deberían establecer un comité directivo específico y un presupuesto exclusivo para la gestión de la ciberseguridad corporativa (Barrero & Bou, 2020).

Otra causa relevante, mencionada por Cano (2021), es el contexto interno, sustentado en la cultura organizacional:

> Cuando se reconoce el reto que implica analizar, estudiar y tratar de transformar una cultura organizacional, particularmente en seguridad de la información, es necesario ir más allá de la práctica estándar de los talleres de concientización, para dar paso a la comprensión de aspectos más profundos de la dinámica empresarial como pueden ser las estructuras de significados de los colectivos, los imaginarios de las personas sobre la temática y aquellos valores explícitos o tácitos que movilizan comportamientos de las personas más allá de cumplir un requisito normativo. (Cano, 2021)

En línea con lo anterior, un estudio realizado en España por Cyber Risk Culture de PricewaterhouseCoopers reveló que el 86 % de las empresas carecen de una cultura de ciberseguridad sólida en el entorno empresarial o deberían mejorarla. "Solo el 27 % de las compañías ya han realizado iniciativas de concientización a la Alta Dirección, mientras que el 68 % tiene planificado o está considerando realizar iniciativas de concientización a la Alta Dirección" (PricewaterhouseCoopers, 2020).

Dado este panorama, se evidencia un problema relacionado con la adopción de una cultura de ciberseguridad en las juntas directivas. Resulta necesario que estos líderes comprendan y aborden la importancia de fortalecer la ciberseguridad en todos los niveles de la organización, lo cual incluye una adecuada evaluación del impacto y las consecuencias de los riesgos asociados.

La cultura de ciberseguridad abarca múltiples componentes, entre los que se incluyen las personas, la tecnología y los procesos. Estos elementos se complementan con cualidades comportamentales que, según su orientación, pueden robustecer o debilitar la ciberseguridad organizacional. En este sentido, la alta dirección, al

constituirse como eje articulador de los distintos procesos organizacionales, debe promover un comportamiento cibernético seguro (Álvarez & Urrego, 2019).

En este contexto, surge una pregunta crucial: ¿cómo generar la adopción de una cultura de ciberseguridad en las juntas directivas? Como tesis, se plantea que dicha adopción es esencial para el cumplimiento efectivo de la estrategia corporativa y para una adecuada gestión del riesgo cibernético. En consecuencia, quienes ocupan cargos directivos deben contar con habilidades que contribuyan al fortalecimiento de la ciberseguridad organizacional, ya que tienen la responsabilidad de articular los procesos institucionales para el logro de los objetivos estratégicos y misionales.

El objetivo de esta investigación es establecer los elementos orientadores que faciliten la adopción de una cultura de ciberseguridad en las juntas directivas, reconociendo que el componente humano es determinante en la conformación de un ecosistema digital seguro. En tanto nivel estratégico de la organización, las juntas directivas deben liderar una estrategia de resiliencia cibernética adecuada, enfocada en la gestión de riesgos de ciberseguridad con el mismo nivel de prioridad con que se abordan los riesgos financieros u otros riesgos organizacionales (NIST, 2023, p. 25).

Cabe destacar que la adopción de una cultura de ciberseguridad puede variar entre organizaciones, en función de factores como el tamaño, el sector industrial y el nivel de madurez en la gestión de riesgos cibernéticos. Por lo tanto, los elementos orientadores aquí propuestos pueden utilizarse como base, según la etapa en la que se encuentre cada organización.

Metodología

Esta investigación se desarrolló a partir de un enfoque cualitativo, que "parte de la premisa de que el mundo social es 'relativo' y sólo puede ser entendido desde el punto de vista de los actores estudiados" (Hernández & Fernández, 2014). Según Vasilachis (2006), la investigación cualitativa se enfoca en el análisis de comportamientos de personas y organizaciones, mediante la recolección de datos y experiencias, que pueden abordarse en cualquier orden (Hernández & Fernández, 2014). Por su parte, la investigación cuantitativa busca "medir y estimar magnitudes de los fenómenos o problemas de investigación" (Hernández & Fernández, 2014, p. 5). En *Estrategias de investigación cualitativa,* Vasilachis (2006) señala que, según Strauss y Corbin, los datos, la interpretación y los escritos constituyen los componentes más relevantes de este tipo de investigación.

Con base en este enfoque, y siguiendo algunas prácticas descritas por Ruiz Olabuénaga (2012), esta investigación se estructuró en las siguientes fases de diseño:

Fase 1: Definición del problema. Se planteó la pregunta de investigación a partir de la identificación de la problemática y su viabilidad de estudio.

Fase 2: Recolección de datos. Se definieron las palabras clave asociadas al objeto de estudio y se realizó la búsqueda de artículos científicos, libros e informes relacionados. La información obtenida se clasificó tras el análisis de los resúmenes (abstracts) y la pertinencia de los documentos. Asimismo, en esta fase se desarrollaron y aplicaron encuestas orientadas a obtener un dato muestral sobre el estado de la cultura de ciberseguridad en juntas directivas.

Fase 3: Análisis de datos. Se procedió a la lectura detallada de los textos seleccionados y al análisis estadístico de los resultados de las encuestas.

Fase 4: Desarrollo de la pregunta de investigación y objetivos. A partir de los hallazgos de la fase anterior, se desarrolló el cuerpo de la investigación, respondiendo a la pregunta planteada y dando alcance a los objetivos, los cuales se abordan en los distintos apartados de este capítulo.

Elementos orientadores para la adopción de una cultura de ciberseguridad a nivel directivo

Este apartado presenta los elementos orientadores que permiten a los integrantes de las juntas directivas reconocer la ciberseguridad como un componente esencial de la estrategia empresarial. La ciberseguridad no puede continuar siendo percibida exclusivamente como una responsabilidad del departamento de TI; por tanto, resulta fundamental comprender no solo los aspectos técnicos, sino también los aspectos culturales organizacionales que favorecen la adopción de una cultura de ciberseguridad sólida en el nivel directivo.

"La alta dependencia de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) traen consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital" (CONPES 3995, 2020, p. 3). Según el *Data Breach Investigation Report 2023,* elaborado por Verizon Business (2023), el 74 % de los incidentes de ciberseguridad tienen origen en errores humanos. Aunque existen soluciones destinadas a proteger a los usuarios y los sistemas tecnológicos frente a ataques cibernéticos, estas cifras evidencian la necesidad de contar con personal capacitado, con

habilidades cibernéticas desarrolladas desde etapas tempranas, que contribuyan a cerrar las brechas vinculadas al comportamiento humano y fomenten una cultura de seguridad digital (González, 2023).

Definición de la cultura de ciberseguridad

De acuerdo con Hofstede (1980), el concepto de cultura contempla cuatro dimensiones que reflejan el comportamiento de los individuos: la *distancia de poder,* que identifica el grado de aceptación de la distribución desigual del poder dentro de una organización; la *evasión de la incertidumbre,* entendida como la resistencia a situaciones ambiguas y la baja tolerancia a ideas o conductas desviadas; el *individualismo frente al colectivismo,* donde el primero refleja un interés centrado en uno mismo y el segundo una cohesión entre grupos internos y externos; y, por último, la *masculinidad,* que indica la orientación de una sociedad hacia valores considerados masculinos, marcando la brecha respecto a los valores femeninos.

En el ámbito investigativo, la cibercultura se define como la interacción compleja entre comunidades humanas, su entorno social, las tecnologías digitales y los medios de comunicación a través de dispositivos computacionales. Esta incluye tres componentes esenciales: cultura del conocimiento, cultura de la información y cultura de la comunicación (González et al., 2007).

La cultura de ciberseguridad se entiende como un conjunto de percepciones, actitudes, valores, suposiciones y conocimientos compartidos en una organización, que determinan su forma de operar y su capacidad para preservar la seguridad de sus activos de información. Este conjunto también tiene como objetivo moldear el comportamiento de los empleados hasta integrarlo como parte de sus *actividades cotidianas* (AlHogail & Mirza, 2014b). Por su parte, la Agencia de Ciberseguridad de la Unión Europea (ENISA, 2017) define la cultura de ciberseguridad organizacional como: "los conocimientos, creencias, percepciones, actitudes, supuestos, normas y valores de las personas en relación con la ciberseguridad y cómo se manifiestan en el comportamiento de las personas con las tecnologías de la información" (p. 7; trad. propia).

A partir de lo anterior, puede afirmarse que el comportamiento de las personas está condicionado por su entorno, las directrices que recibe y su percepción respecto a la interacción con la sociedad. En consecuencia, la adopción de una cultura de ciberseguridad en las organizaciones depende de las exigencias impuestas por un comportamiento considerado aceptable tanto por el grupo como por el entorno organizacional.

Importancia de la cultura de ciberseguridad

La cuarta revolución industrial y el proceso de transformación digital avanzan a un ritmo acelerado, generando desafíos significativos en materia de ciberseguridad, como la hiperconectividad de los sistemas, que da lugar a brechas de seguridad considerables y que deben ser abordadas desde múltiples perspectivas (Schwab, 2016). Uno de los principales riesgos en este contexto está relacionado con el comportamiento humano y el manejo de la información y los sistemas tecnológicos. Diversos estudios sobre cultura de seguridad concluyen que los *insiders* representan una amenaza latente para los activos de información de las organizaciones (AlHogail & Mirza, 2014a).

El informe de IBM Security indica que "las organizaciones con un alto nivel de escasez de habilidades de seguridad tuvieron un costo promedio de 5,36 millones de dólares" (IBM Security, 2023, p. 29), que representa un 30 % más en comparación con aquellas que poseen una postura y conocimientos más sólidos en ciberseguridad.

Esto muestra la importancia de fomentar una cultura de ciberseguridad dentro de las organizaciones, ya que permite mitigar los riesgos a los que estas se encuentran expuestas, en particular los derivados de comportamientos inadecuados por parte de sus colaboradores. Da Veiga y Eloff (2010) destacan que las "organizaciones requieren orientación para establecer una cultura de seguridad de la información" y que "necesitan medir e informar sobre el estado de seguridad de la información en la organización" (p. 1).

Asimismo, el análisis documental realizado por Uchendu et al. (2021) identificó un conjunto significativo de estudios (34 en total) que coinciden en que el apoyo, liderazgo y participación de la alta dirección es un factor fundamental para el desarrollo de una cultura organizacional de ciberseguridad (Uchendu et al., 2021).

En esta misma línea, AL-sartawi (2020) resalta "la importancia de nombrar a miembros de junta directiva con conocimientos y experiencia en TI", dado que esto favorece la toma de decisiones más adecuadas frente a amenazas y desafíos cibernéticos (p. 1). Esta recomendación refuerza la necesidad de consolidar una cultura de ciberseguridad robusta.

Estudios de caso y ejemplos prácticos

Los siguientes casos ilustran la importancia de desarrollar una cultura de ciberseguridad organizacional como estrategia para reducir riesgos, mediante la concientización del personal.

Cómo Yahoo construyó una cultura de ciberseguridad

De acuerdo con Pearlson et al. (2021), el grupo de investigación Sloan (CAMS) del MIT colaboró con Yahoo en la implementación de mecanismos para fortalecer su cultura de ciberseguridad. Inicialmente, se conformaron tres equipos con funciones específicas para promover la participación proactiva de los empleados: uno con capacidades técnicas, encargado de evaluar sistemas, servicios, procesos y personal para detectar vulnerabilidades; un segundo equipo, enfocado en la concientización en seguridad; y un tercero, especializado en ingeniería del comportamiento.

Durante el proceso, se distinguieron las diferencias entre acciones, hábitos y comportamientos, lo que permitió establecer objetivos de comportamiento como punto de partida para la implementación de medidas de cambio. A través del desarrollo de competencias y la introducción de incentivos, se logró modificar el comportamiento de los empleados, consolidando una cultura de ciberseguridad sólida.

Determinación de la madurez de la cultura de ciberseguridad organizacional

El estudio "Determining cybersecurity culture maturity and deriving verifiable improvement measures", realizado por Dornheim y Zarnekow (2023), evaluó el nivel de madurez de la cultura de ciberseguridad en una organización utilizando el marco propuesto por Da Veiga y Eloff (2010). Este marco se basa en seis dimensiones fundamentales que conforman el modelo de evaluación de la cultura en la protección de la información (IPCA), orientadas a medir "cómo los empleados perciben la protección de la información desde una perspectiva de ciberseguridad" (Dornheim & Zarnekow, 2023, p. 6; trad. propia).

El estudio, basado en encuestas aplicadas en dos momentos diferentes a una amplia muestra del personal, reveló que las dimensiones con mayores necesidades de desarrollo eran: 1) responsabilidad en materia de ciberseguridad, 2) compromiso en ciberseguridad y 3) efectividad de las políticas de ciberseguridad. Uno de los principales retos identificados fue aumentar el nivel de compromiso, dado que muchos empleados consideraban la ciberseguridad como un asunto trivial. Esta percepción motivó el diseño de una campaña dirigida a convencer a los directivos sobre la importancia estratégica de la ciberseguridad, desde donde se generó la comunicación hacia el resto del personal.

Adicionalmente, se llevaron a cabo actividades dirigidas tanto a empleados como a directivos y ejecutivos, entre las que se incluyeron talleres prácticos sobre el uso de herramientas de *phishing* y la clonación de sitios web, con el fin de demostrar la facilidad con la que puede ejecutarse un ciberataque.

Responsabilidades de la junta directiva en la creación de una cultura de ciberseguridad

El rol de la junta directiva puede interpretarse desde dos enfoques diferenciados: uno pasivo y otro activo. El enfoque pasivo está basado en una estructura jerárquica en la que el poder se concentra en el gerente general y el presidente, mientras que la junta se limita a aprobar la estrategia definida por el equipo gerencial. En contraste, el enfoque activo contempla a los miembros de la junta como pensadores independientes y autónomos en la definición de la dirección estratégica de la organización, aunque comparten con la gerencia la responsabilidad de cumplir con los objetivos organizacionales (Azuero et al., 2020).

Actualmente, los altos directivos enfrentan una creciente frecuencia de ataques cibernéticos. De acuerdo con el equipo de Advice Group LATAM (2023), los tipos de ataque más comunes incluyen el *phishing* (44 %), estafas o *scamming* (33 %), *spyware* o *malware* (22 %) y *ransomware* (20 %). Pese a este panorama, los miembros de las juntas directivas consideran que no están preparados para hacer frente a un ataque cibernético. Una encuesta aplicada a 600 miembros de juntas directivas reveló que el 65 % considera que sus organizaciones están en riesgo de ser víctimas de un ciberataque en el corto plazo (Milică & Pearlson, 2023). Asimismo, el Foro Económico Mundial indica que el 95 % de los problemas de ciberseguridad se originan en errores humanos (World Economic Forum, 2022).

Frente a este contexto, la junta directiva debe asumir un papel de liderazgo en la promoción de la cultura de ciberseguridad a todos los niveles de la organización. Esto implica la identificación de responsabilidades, la supervisión de la seguridad organizacional y la implementación de cambios cuando sea necesario (Maurer et al., 2020). Este compromiso debe incluir la asignación de recursos humanos y de infraestructura para garantizar la implementación y el mantenimiento de medidas de ciberseguridad. Sin embargo, la sola disposición de estos elementos no resulta suficiente. Las organizaciones deben garantizar su operatividad mediante la conformación de un comité directivo específico y la asignación de un presupuesto exclusivo para la gestión de la ciberseguridad (Barrero & Bou, 2020).

ENISA (2017) señala que la alta dirección tiene la responsabilidad directa en materia de ciberseguridad, la cual debe entenderse como una fuente para la toma de decisiones estratégicas. Esta debe considerarse una inversión destinada a la reducción de riesgos asociados a pérdidas financieras, daño reputacional, sanciones legales por incumplimiento normativo y exigencias de los accionistas:

> Para cambiar la cultura, la alta dirección debe utilizar una serie de instrumentos, como las declaraciones de valores, la comunicación interna, la educación, y debe predicar con el ejemplo a través de sus comportamientos en apoyo de sus declaraciones visionarias. (ENISA, 2017, p. 32)

La OEA (2019) señala que "no es responsabilidad de la junta convertirse en expertos en TI, pero la junta debe saber qué preguntas hacerles a los departamentos de TI" (p. 8). Así, se debe establecer un seguimiento periódico para asegurar que los responsables mantengan los controles de ciberseguridad necesarios para la operación de la organización.

De manera complementaria, la Asociación Nacional de Directores de Empresas (NACD, por sus siglas en inglés) enfatiza la necesidad de contar con un modelo sostenible, empezando por un compromiso de la alta dirección que promueva una cultura de ciber-responsabilidad. Esta debe incluir una gestión efectiva del riesgo cibernético, reconociendo que los miembros de las juntas directivas poseen un poder único para garantizar que los Oficiales de Seguridad de la Información (CISO) dispongan de la influencia y los recursos adecuados para liderar la estrategia de ciberseguridad a nivel corporativo (Clinton et al., 2023).

En el contexto latinoamericano, el documento CONPES 3995 (2020) recomienda el desarrollo de programas de formación para niveles directivos y ejecutivos, con el objetivo de dotarlos de las competencias necesarias para gestionar los riesgos en seguridad digital.

Los ejecutivos deben asumir un rol activo en la integración de la cultura de ciberseguridad, adecuándola a sus perspectivas y necesidades, de modo que puedan reconocer y responder adecuadamente a una realidad transformada por los riesgos emergentes en este ámbito (Cano, 2023).

Uno de los principales desafíos en la consolidación de una cultura de ciberseguridad en las juntas directivas es la falta de concientización. Esta se manifiesta en la carencia de preparación para tomar decisiones informadas, lo que impide dimensionar de forma adecuada el impacto y las consecuencias de los riesgos cibernéticos dentro de las organizaciones.

Las causas identificadas para la limitada adopción de una cultura de ciberseguridad en las juntas directivas son las siguientes:

- *Falta de previsión sobre las consecuencias de la ciberseguridad como riesgo latente.* Para supervisar adecuadamente este tipo de riesgos, es imprescindible que comprendan las responsabilidades que les competen, ya que la toma de decisiones en esta materia no puede ser delegada a estructuras operativas (Clinton et al., 2023).

- *Ausencia de un ecosistema digital robusto o insuficiente presupuesto.* La inversión adecuada es esencial para enfrentar los desafíos de ciberseguridad. De acuerdo con un informe de PricewaterhouseCoopers (2020), solo el 9 % del presupuesto de seguridad de la información de las empresas se destina a actividades de formación y concientización para fortalecer una cultura de ciberseguridad.
- *Percepción de la ciberseguridad como un tema exclusivamente tecnológico.* En la encuesta de la OEA (2018) sobre protección de infraestructuras críticas en América Latina y el Caribe, el 42 % de los encuestados indicó que los esfuerzos de ciberseguridad son supervisados por el departamento de TI. Solo el 13 % señaló que dicha responsabilidad recae en el nivel C-Level, y apenas un 4 % mencionó a otras áreas como encargadas de esta función (OEA, 2018, p. 38).

La falta de reconocimiento del alcance estratégico de la ciberseguridad, la escasa inversión y la limitada conciencia sobre los impactos de los riesgos cibernéticos pueden convertirse en una ventaja para los atacantes, quienes se aprovechan de estas debilidades para obtener beneficios.

Así, esta investigación busca identificar aquellos elementos que favorecen la generación de una cultura de ciberseguridad en los que las juntas directivas deben enfocarse en cuanto a ciberseguridad.

Elementos orientadores para una cultura de ciberseguridad

Para establecer elementos orientadores que guíen de manera eficaz la cultura de ciberseguridad en las juntas directivas, resulta fundamental identificar las características propias de este grupo de líderes que pueden actuar como catalizadores en la adopción rápida y efectiva de prácticas en este ámbito. Álvarez y Urrego (2019) introducen los criterios básicos de éxito (CSF), como componentes esenciales que favorecen el desarrollo organizacional y el logro de objetivos. Estos criterios incluyen la confianza, los sistemas de información, la comunicación intraorganizacional, la estructura organizativa y los mecanismos de incentivos, todos los cuales contribuyen a una transferencia efectiva del conocimiento en ciberseguridad.

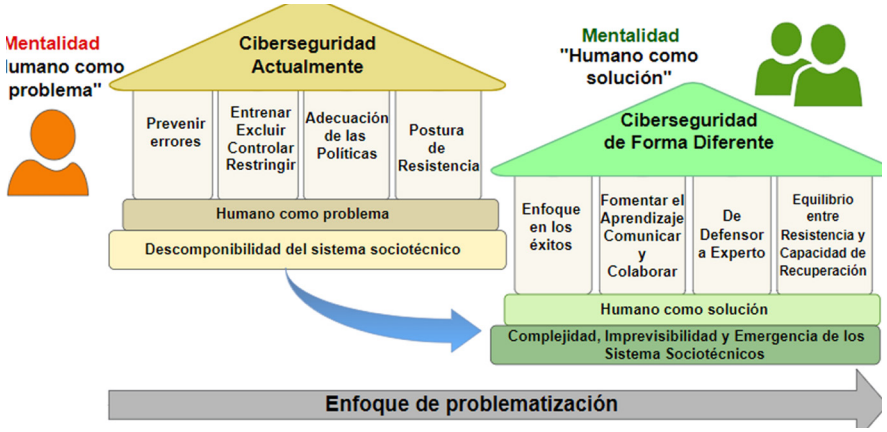
Diferentes elementos conforman el andamiaje necesario para una cultura de ciberseguridad que promueva comportamientos preventivos dentro de la organización. Entre ellos, el factor humano se destaca como un recurso estratégico de

alto valor. En este sentido, Zimmermann y Renaud (2019) proponen un cambio de paradigma al afirmar que:

> La mentalidad "diferente" reconoce la capacidad del ser humano bien intencionado para ser un contribuyente importante a la ciberseguridad organizacional, así como su potencial para ser "parte de la solución" en lugar de "el problema". En esencia, este nuevo enfoque trata inicialmente a todos los humanos en el sistema como si fueran bien intencionados. (p. 168; trad. propia)

Aunque tradicionalmente el ser humano ha sido percibido como el eslabón más débil en la cadena de seguridad de la información, es precisamente en este punto donde debe invertirse dicha percepción. En lugar de concebirlo como una amenaza, debe ser reconocido como un agente clave capaz de robustecer la cultura de ciberseguridad (figura 1).

Figura 1. *El ser humano como problema; el ser humano como solución.*



Fuente: Elaboración propia con base en Zimmermann y Renaud (2019, p. 179)

Con este contexto, el ser humano se define como un elemento crítico en materia de ciberseguridad. Por tanto, resulta esencial establecer los elementos necesarios para fomentar una cultura de ciberseguridad en las juntas directivas, mediante la implementación de políticas adecuadas y la generación de conciencia. Reconocer al ser humano como un componente clave de esta cultura implica un cambio de perspectiva, en el cual su intervención se concibe como un aspecto positivo y de la cultura de ciberseguridad.

En consecuencia, se seleccionaron tres referentes teóricos que identifican elementos esenciales para el desarrollo de una cultura de ciberseguridad sólida:

ENISA, Isabella Corradini y PricewaterhouseCoopers Asesores de Negocios. Estos autores abordan el tema desde una perspectiva integral que promueve la sinergia entre personas, procesos y tecnología.

De acuerdo con ENISA (2017), una cultura de ciberseguridad eficaz requiere la adopción de un enfoque adecuado que fortalezca la resiliencia de los activos de información. Para ello, identifica elementos clave como los conocimientos, creencias, percepciones, actitudes, suposiciones, normas y valores.

De manera complementaria, Corradini (2020) agrupa los elementos de la cultura organizacional en tres categorías fundamentales: artefactos, valores y supuestos básicos, subdivididos a su vez en concientización, valores y principios, comportamiento. Señala también la relevancia del conocimiento en seguridad de la información.

Por su parte, PricewaterhouseCoopers (2020) propone cuatro dominios principales para evaluar el nivel de cultura de ciberseguridad en las organizaciones: estrategia, conocimiento, comportamiento y perspectiva futura.

En la tabla 1 se presentan los criterios identificados por cada autor, los cuales constituyen la base para el desarrollo de una guía orientadora en la adopción de una cultura de ciberseguridad desde las juntas directivas.

Tabla 1. *Elementos orientadores para establecer una cultura de ciberseguridad*

Autor	Elementos
ENISA (2017)	Conocimientos
	Creencias
	Percepciones
	Actitudes
	Suposiciones
	Normas
	Valores
Isabella Corradini (2020)	Concientización
	valores y principios
	Interacción con la tecnología
	Comportamiento
	Conocimiento
Pricewaterhouse Coopers Asesores de Negocios, S.L. (2020)	Estrategia
	Conocimiento
	Comportamiento
	Perspectiva futura

Fuente: Elaboración propia

Como resultado del análisis realizado y documentado en la tabla 1, se evidencia la coincidencia de varios elementos entre los autores. Por tanto, para efectos de esta investigación se seleccionaron los elementos orientadores conocimiento, normas, valores, concientización, estrategia y comportamiento, considerados como claves para establecer una guía integrada que permita abordar de manera efectiva la cultura de ciberseguridad en la organización, enfocándose en los miembros de juntas directivas como líderes de la estrategia de ciberseguridad corporativa.

Estos elementos orientadores se toman como base debido a la relevancia que les atribuyen los autores, por lo que los miembros de las juntas directivas deberán identificar cómo se alinean con los valores y estrategias propias de sus organizaciones para el establecimiento de una cultura de ciberseguridad corporativa. Estas validaciones pueden realizarse mediante cuestionamientos que permitan determinar si la junta requiere actualizaciones periódicas en materia de ciberseguridad a través de expertos en la materia. Asimismo, resulta pertinente que los miembros de las juntas incorporen en sus conversaciones datos relevantes sobre ciberseguridad que puedan impactar a la organización, analizando cómo las decisiones comerciales contemplan los riesgos cibernéticos. Una alternativa adicional para mantenerse actualizados consiste en asistir a conferencias especializadas o en optar por certificaciones que fortalezcan su conocimiento en ciberseguridad.

En el siguiente acápite se contrastan los elementos orientadores con los criterios evaluadores que permiten identificar el nivel de familiarización de los miembros de las juntas directivas con las capacidades humanas, administrativas y tecnológicas necesarias para la adopción de una cultura de ciberseguridad.

Criterios evaluadores para medir el nivel de cultura de ciberseguridad en juntas directivas

La ciberseguridad ha adquirido un espacio relevante y urgente como componente estratégico en las organizaciones, por lo que la adopción y el compromiso hacia una cultura de ciberseguridad deben comenzar desde los niveles más altos de la estructura organizativa. Las juntas directivas, en tanto responsables de definir el rumbo estratégico de las organizaciones, deben integrar y fortalecer esta cultura para su adopción en todos los procesos.

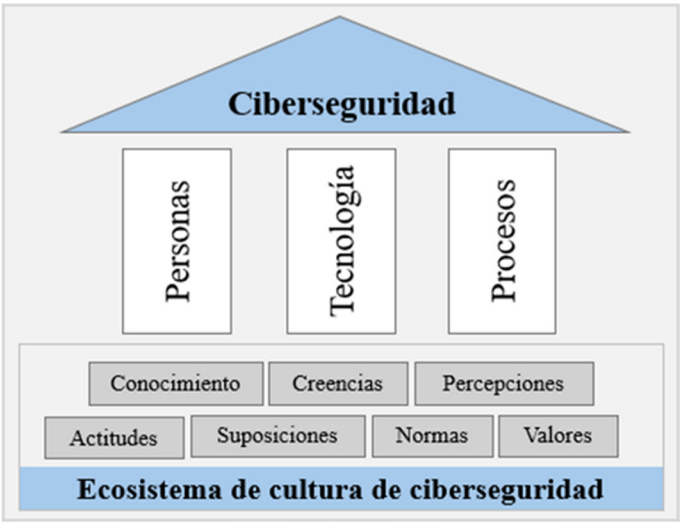
La ciberseguridad se sustenta en tres pilares fundamentales: *personas, tecnología* y *procesos,* los cuales son interdependientes y deben funcionar

de manera armónica para el fortalecimiento de una cultura de ciberseguridad (PricewaterhouseCoopers, 2020). Estos pilares se relacionan directamente con las *capacidades humanas, tecnológicas y administrativas* de cada organización.

Definición e importancia de los criterios evaluadores

Establecer una cultura de ciberseguridad implica desarrollar un ecosistema que la respalde, fundamentado en los pilares de personas, tecnología y procesos (Álvarez & Urrego, 2019) (figura 2).

Figura 2. *Ecosistema de cultura de ciberseguridad.*



Fuente: Álvarez y Urrego (2019).

En primer lugar, se encuentran las personas, por lo que la concientización y capacitación resultan fundamentales para mitigar el error humano, considerado la causa más común de fallas tecnológicas relacionadas con la ciberseguridad (Steele, 2024).

Los procesos constituyen el soporte para establecer políticas y procedimientos destinados a proteger la información, basándose en el cumplimiento de normas, estándares y buenas prácticas, y asegurando que los empleados estén alineados con dichas políticas (Da Veiga & Eloff, 2010).

La tecnología, por su parte, respalda el aseguramiento de la información; no obstante, debe garantizarse la generación de conocimiento respecto al uso

adecuado de las herramientas de TI, de modo que se mantengan alineadas con las necesidades de la organización y actualizadas para prevenir amenazas emergentes. En este sentido, resulta crucial considerar cómo la organización construye valores, conocimientos y comportamientos basados en el uso de las herramientas tecnológicas (AlHogail & Mirza, 2014a).

Estos pilares se consolidan como criterios o capacidades —humanas, administrativas y tecnológicas— orientadoras para proteger la información y generar un ambiente de cibercultura resiliente.

Métodos de evaluación

En el marco de este proyecto de investigación, se llevó a cabo una encuesta destinada a evaluar el nivel de cultura organizacional en materia de ciberseguridad entre miembros de juntas directivas, roles de C-Level, Oficiales de Seguridad de la Información y Gerentes de diversas empresas. A través de esta herramienta se recopilaron datos esenciales de dieciséis participantes pertenecientes a los roles mencionados, conforme se detalla en la tabla 2. Se utilizó un sistema de encuesta semiestructurada por conveniencia, dada la identificación previa de los actores relevantes cuyas respuestas resultaban fundamentales para el desarrollo del ejercicio.

La encuesta incluyó el consentimiento informado, en cumplimiento de lo dispuesto en la Ley 1581 de 2012 y en el Decreto 1377 de 2013. Asimismo, se dejó a voluntad de los encuestados el registro de sus nombres, apellidos y la identificación de la organización a la que pertenecen.

La encuesta se enfocó en medir la comprensión de los participantes respecto a las capacidades humanas, administrativas y tecnológicas de sus organizaciones, alineadas a los elementos orientadores previamente definidos.

Tabla 2. *Participantes por roles*

Rol	Cantidad
Chief information and security officer (CISO)	7
Integrante de junta directiva	4
Director de área	3
Chief executive officer (CEO)	2

Fuente: Elaboración propia.

Capacidades humanas

Ante la pregunta: ¿Qué entiende por cultura de ciberseguridad?, el 75 % de los encuestados asoció el concepto con la adopción de un conjunto de valores, actitudes y buenas prácticas para proteger sus sistemas, redes y datos frente a amenazas cibernéticas. Por su parte, el 25 % relacionó el término más directamente con los procedimientos y tecnologías destinadas a garantizar la confidencialidad, integridad y disponibilidad de la información. Este resultado evidencia la necesidad de implementar programas de concientización y fortalecer el conocimiento en todos los niveles de la organización, comenzando por los miembros de juntas directivas y los cargos ejecutivos.

Una manera de evaluar los esfuerzos de las organizaciones por mejorar la comprensión de la cultura de ciberseguridad es validar la frecuencia con la que se realizan campañas en torno a este tema. Como resultado, el 19 % indicó que se hacen anualmente, otro 19 % señaló que se realizan semestralmente, el 56 % respondió que son llevadas a cabo trimestralmente y el 6 % indicó que no se hacen. Estas respuestas demuestran que, en su mayoría, las organizaciones manifiestan un interés por promover el conocimiento sobre cultura de ciberseguridad a través de campañas periódicas.

Una validación importante en esta investigación fue conocer cómo se perciben las responsabilidades en la organización. Para ello, se formuló la siguiente pregunta: ¿Considera que la ciberseguridad es una responsabilidad del área de TI/Tecnología? El 25 % respondió afirmativamente, mientras que el 75 % consideró que no lo es. Aunque la mayoría no atribuye la responsabilidad exclusivamente al área tecnológica, preocupa que aún exista un porcentaje que sí lo hace. Esta percepción constituye una de las variables identificadas como parte del problema y refleja la necesidad de un cambio de perspectiva.

La creencia de que el área de TI es la principal responsable puede estar relacionada con la asociación directa del término *ciberseguridad* con aspectos tecnológicos, dejando de lado el componente conductual y la responsabilidad individual que implica la toma de decisiones en esta materia.

Dentro de la medición de cultura de ciberseguridad se buscó identificar si existe un plan de capacitación en esta materia dirigido a los miembros de la junta directiva en sus organizaciones. Los resultados muestran que solo el 56 % de los miembros ha recibido algún tipo de capacitación, mientras que el 44 % no ha sido capacitado.

Este hallazgo pone en evidencia la urgencia de que los miembros de juntas directivas desarrollen una conciencia sólida en torno a la ciberseguridad, que les

permita contar con herramientas cognitivas adecuadas para la toma de decisiones acertadas al respecto.

Como parte de las validaciones realizadas, se investigó lo siguiente: Si su organización ya cuenta con una implementación de cultura de ciberseguridad, ¿cuál considera que fue el reto más complicado de abordar?

El 31 % identificó como principal reto la definición de la estrategia para la implementación de la cultura de ciberseguridad; otro 31 % señaló la asignación de presupuesto para disponer de los recursos necesarios. El 19 % consideró que el mayor desafío fue el gobierno en la definición del modelo de cultura de ciberseguridad, mientras que el 13 % indicó como dificultad la evaluación de la madurez y del comportamiento en torno a dicha cultura. Finalmente, el 6 % manifestó no contar aún con una implementación de cultura de ciberseguridad.

Capacidades administrativas

Las organizaciones deben proveer los recursos necesarios para la ciberseguridad. Con el objetivo de identificar si esta condición se cumple, se planteó la siguiente pregunta: ¿Qué área se encarga de la ciberseguridad en su organización?

El 63 % de las respuestas indicó que esta responsabilidad recae en el área de TI, el 19 % señaló al área de riesgo y cumplimiento, un 6 % mencionó el área de seguridad, otro 6 % indicó la dirección de sistemas de información y el 6 % restante señaló al proceso de continuidad del negocio como encargado. Con estos resultados, se observa que el área de TI concentra una alta asignación de responsabilidades en la gestión de la ciberseguridad.

La siguiente validación se realizó para obtener una aproximación sobre la relevancia de la ciberseguridad en las organizaciones, determinando: ¿Qué porcentaje del presupuesto anual está destinado a la ciberseguridad en su organización?

Los resultados revelan una cifra que sustenta una de las causas de la problemática de esta investigación, relacionada con la ausencia de un ecosistema digital o el bajo presupuesto asignado en las organizaciones. El 38 % de los encuestados indicó que se destina menos del 5 % del presupuesto; el 19 % señaló una asignación entre el 5 % y el 10 %; el 25 % informó que el presupuesto asignado está entre el 10 % y el 20 %, y ningún encuestado reportó asignaciones superiores a este rango. Solo el 6 % indicó que el presupuesto asignado supera el 20 %, mientras que el 13 % manifestó desconocer la cifra correspondiente a su organización.

Se planteó un interrogante con el fin de determinar si se están gestionando de manera adecuada los riesgos cibernéticos: ¿La junta directiva tiene conocimiento

de los riesgos cibernéticos a los que está expuesta la organización y de las posibles consecuencias en términos legales, financieros, operacionales y/o reputacionales?

El 81 % de los encuestados respondió afirmativamente, el 13 % indicó no estar seguro/a y el 6 % manifestó no conocer los riesgos cibernéticos. Este último resultado confirma que algunos integrantes de las juntas directivas toman decisiones para la organización sin tener conciencia del impacto que podría generar la materialización de un riesgo cibernético. Esta validación resulta relevante para conocer las tendencias organizacionales, como una forma de apoyar y mantener actualizados los planes y protocolos de contingencia definidos frente a las amenazas cibernéticas.

Ante la pregunta: ¿Se incluye a la junta directiva en el proceso de toma de decisiones durante incidentes cibernéticos críticos o de alto nivel? El 56 % respondió que siempre, el 25 % indicó que ocasionalmente y el 19 % manifestó que nunca se incluye a la junta para este tipo de decisiones. Esta actividad cobra gran relevancia, ya que, aunque los directivos no deben ser expertos técnicos, sí deben contar con las capacidades generales necesarias para identificar el impacto que un incidente cibernético puede generar en términos legales, económicos o de afectación a la imagen organizacional.

En línea con la pregunta anterior, se investigó lo siguiente: ¿Ha participado en algún ejercicio de simulación de riesgo cibernético en donde la junta directiva deba tomar decisiones frente a un incidente cibernético? El 69 % respondió no haber participado, el 25 % indicó que sí ha participado y el 6 % señaló que, aunque no ha participado, sí ha estado informado. La colaboración de la junta directiva en este tipo de simulaciones proporciona una visión general sobre cuál debería ser su enfoque ante un incidente o la materialización de un riesgo cibernético real.

Capacidades tecnológicas

Respecto a las capacidades tecnológicas, se indagó lo siguiente: ¿Conoce si su organización cuenta con las herramientas tecnológicas y procedimientos necesarios para una adecuada gestión de la ciberseguridad? El 81 % de los encuestados indicó que sí cuentan con herramientas para una adecuada gestión de la ciberseguridad, mientras que el 19 % señaló que no disponen de las herramientas necesarias para su debida gestión.

Frente a la postura de ciberseguridad de su organización, se planteó la siguiente pregunta: ¿Conoce cuáles son los índices de seguridad de sus socios estratégicos o proveedores y cómo podrían impactar a su organización en caso de que estos sufran un incidente cibernético?

El 56 % indicó conocer algunos índices de seguridad de sus terceros, pero no de todos; solo el 6 % conoce el detalle y cómo podría afectarle a su organización; el 19 % tiene una idea general, pero no conoce el detalle ni el impacto que un incidente cibernético de un tercero podría generar; el 13 % señaló que la gestión de la ciberseguridad es manejada por otro departamento o equipo en la organización; y el 6 % manifestó desconocer los índices de seguridad de sus socios o terceros. Dado el resultado de esta pregunta, se infiere que, al delegar la responsabilidad de la gestión de la ciberseguridad en otras áreas, la junta directiva cede su obligación de reconocer la exposición a los riesgos cibernéticos.

Con base en las respuestas anteriores, se identifica que el *conocimiento*, los *valores* y la *concientización* forman parte de los componentes presentes en las juntas directivas. El conocimiento permite que las personas comprendan las reglas, funciones y comportamientos necesarios para la toma de decisiones informadas. A su vez, promover un comportamiento alineado con los valores de la organización facilita que los colaboradores adopten dichos valores en sus actividades cotidianas, mientras que la concientización en ciberseguridad se ha ido normalizando en las organizaciones.

A pesar de esto, los elementos de *norma, estrategia* y *comportamiento* no muestran aún un nivel de madurez suficiente y requieren un mayor fortalecimiento en las juntas directivas, según las respuestas obtenidas. Por ejemplo, la inversión en ciberseguridad depende de la autonomía de cada organización, ya que no existe una normatividad que exija destinar un porcentaje específico del presupuesto anual a este aspecto.

Por otra parte, uno de los retos más difíciles de abordar en las organizaciones es el desarrollo de una estrategia efectiva para la formación y concientización en cultura de ciberseguridad. En cuanto al comportamiento, se observa que las responsabilidades en temas de ciberseguridad recaen usualmente sobre el área de TI, y aunque la junta directiva es incluida en el proceso de toma de decisiones durante incidentes cibernéticos críticos, no siempre cuenta con la preparación necesaria que le permita actuar con mayor experticia en este campo.

Estudio de caso

Onumo et al. (2021), en su investigación aplicada a tres empresas, desarrollaron un modelo combinando teorías relacionadas con el comportamiento planificado, valores competitivos, y los factores tecnológicos, organizacionales y ambientales, con el fin de validar los valores culturales asociados a los mecanismos adoptados

por los empleados. Como resultado, identificaron que el comportamiento de las personas se asocia directamente a los elementos organizacionales y a los procesos, mientras que las creencias se ven moderadas por las tecnologías de información. Onumo et al. (2021) señala como un desafío las múltiples interpretaciones de la cultura de seguridad en la literatura, por lo que invita a considerar cómo los factores organizacionales, los mecanismos de comportamiento y el entorno tecnológico pueden persuadir e influir en las personas.

Con base en los resultados obtenidos en esta investigación, se destacan en la figura 3 los elementos que están implícitos o que requieren fortalecimiento en las juntas directivas para la adopción de una cultura de ciberseguridad. Estos elementos demandan la promoción de una mentalidad de seguridad proactiva. Asimismo, es fundamental que las juntas directivas impulsen la formación continua en ciberseguridad y establezcan mecanismos de vigilancia y evaluación que aseguren que las acciones implementadas se mantengan actualizadas y eficaces ante las amenazas emergentes.

En este sentido, vale la pena resaltar que los directivos deben validar y fomentar la cultura de ciberseguridad en sus organizaciones, basándose en las capacidades y elementos que les permitan fortalecer su resiliencia frente a incidentes cibernéticos.

Figura 3. *Estado de apropiación de los elementos necesarios para una cultura de ciberseguridad en las juntas directivas.*

Fuente: Elaboración propia.

Guía de elementos y pasos para adoptar una cultura de ciberseguridad en juntas directivas

Las juntas directivas, debido a su rol relevante en las organizaciones, deben impulsar las políticas e inclinarse por mantener una estrategia que fomente una cultura de ciberseguridad sólida. Se requiere un compromiso adecuado por parte de las juntas directivas, donde sus capacidades conduzcan a la organización y a todos sus integrantes hacia un nivel adecuado de concientización en temas de ciberseguridad (Cyber Citadel, 2023).

De acuerdo con lo desarrollado en el acápite anterior, en el cual se identificaron los elementos que están implícitos en las organizaciones y que contribuyen al desarrollo de la cultura cibernética, también se evidenciaron algunos aspectos que deben ser fortalecidos para estructurar de manera adecuada las capacidades y aptitudes de los miembros de la junta directiva como estrategas y líderes en la implementación de la ciberseguridad organizacional.

En este acápite se detallan los elementos que guiarán a los directivos en la adopción de una cultura de ciberseguridad, la cual podrá extenderse posteriormente a toda la organización. Estos elementos se apoyan en sus respectivos pasos, que brindan recomendaciones clave para su implementación. Finalmente, se presentan algunas preguntas de reflexión que pueden ser útiles antes y durante el proceso de desarrollo de una cultura de ciberseguridad.

Estrategia

De acuerdo con PricewaterhouseCoopers (2020), la estrategia debe enfocarse en aumentar las capacidades existentes en la junta directiva y profundizar en la concientización sobre el impacto de la ciberseguridad en la organización. La estrategia para desarrollar una cultura de ciberseguridad debe considerar la importancia de vincular a las personas, la tecnología y los procesos. Las personas, como recurso primordial, deben incluirse en planes específicos que contemplen temas como la gestión de incidentes cibernéticos y la toma de decisiones ante la materialización de riesgos de ciberseguridad.

Según Giraldo Ríos (2024), "las empresas deben considerar la estrategia como un todo y empezar a implementarla o corregirla gradualmente, según su ritmo de adaptación" (p. 19). Contar con una estrategia permitirá, a su vez, conocer la postura de la organización frente a la ciberseguridad y facilitar la construcción del programa de concientización (Schneider et al., 2020).

El desarrollo de la estrategia debe contemplar varios pasos que orienten una implementación ordenada. Con base en la literatura estudiada, se proponen los siguientes pasos para desarrollar el elemento orientador *Estrategia.*

Paso 1. Medir el nivel de madurez en cultura de ciberseguridad de la junta directiva

La adopción de una cultura de ciberseguridad debe ser una tarea medible, y uno de los mecanismos para ello es la utilización de un modelo de madurez que permita identificar fortalezas y aspectos de mejora en su implementación y mantenimiento a lo largo del tiempo.

Diversos autores han diseñado marcos aplicables desde distintas perspectivas, entre los cuales se encuentran modelos para determinar comportamientos orientados a la seguridad de la información, cumplimiento de políticas de seguridad de la información, medición de la apropiación de la cultura de ciberseguridad organizacional (AlHogail & Mirza, 2014a; Da Veiga & Eloff, 2010; Da Veiga & Martins, 2015), así como modelos centrados en las personas, como el propuesto por Hayden (2016) (tabla 3).

Tabla 3. *Marcos y modelos de medición de cultura de seguridad de la información y ciberseguridad*

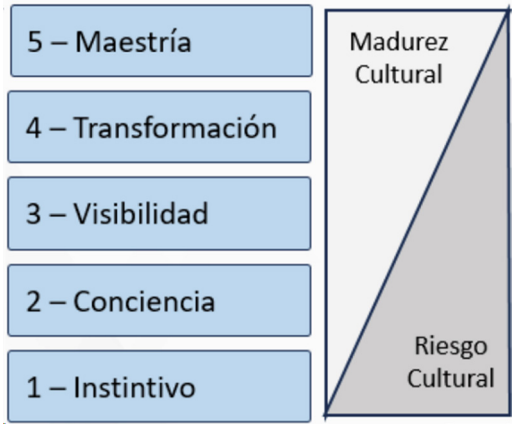
Autor	Marco / modelo	Enfoque
Da Veiga y Eloff (2010)	Information Security Culture Framework (ISCF)	Cultura en seguridad de la información.
Da Veiga y Eloff (2010)	Information Security Culture Assess-ment (ISCA)	Cultura en seguridad de la información
Da Veiga y Martins (2015)	Information security culture and information protection culture: A validated assessment instrument	Cultura en seguridad de la información.
Hogail (2015)	The Information Security Culture Framework (ISCF)	Cultura en seguridad de la información
Hayden (2016)	Competing Security Cultures Framework (CSCF)	Cultura de seguridad y adopción de comportamientos de seguridad
Hayden (2016)	Culture Capabilities Maturity Model (CCMM)	Identificación de capacidades culturales en las personas de una organización

Fuente: Elaboración propia.

De los documentos antes descritos, se concluye que el modelo presentado por Hayden (2016) tiene un enfoque más cercano al propósito de esta investigación,

ya que puede ser aplicado directamente a los miembros de la junta directiva para determinar sus fortalezas y aspectos de mejora. El modelo de madurez de capacidades de cultura (CCMM) describe cinco niveles y se divide en dos estados transversales: uno identificado como cultura de riesgo, en el cual las personas actúan instintivamente y de manera reactiva sin comprender cómo funciona la organización, y otro en el nivel superior, donde la organización entiende el comportamiento de las personas hasta el punto de poder modificarlo con rapidez y eficacia para enfrentar cualquier reto (Hayden, 2016) (figura 4).

Figura 4. *El modelo de madurez de capacidades de cultura.*



Fuente: Adaptado de Hayden (2016).

Existen estudios como el de Dornheim y Zarnekow (2023), quienes utilizaron el modelo de Da Veiga y Eloff para determinar la madurez en cultura de ciberseguridad en una compañía australiana, demostrando que los marcos pueden ser adaptados a las necesidades de cada organización.

Paso 2. Designar los recursos necesarios para la gestión de la ciberseguridad

La evolución de las ciberamenazas requiere que los miembros de las juntas directivas asuman un mayor compromiso con la ciberseguridad de sus organizaciones (Nodehi et al., 2024), asegurando la resiliencia corporativa y reduciendo los riesgos identificados a través de ejercicios de evaluación. Por ello, la asignación de recursos, tanto técnicos como humanos, resulta necesaria tanto para el desarrollo de la ciberseguridad organizacional como para la adopción de la cultura de ciberseguridad entre sus miembros (ENISA, 2017).

Concientización

La concientización comprende tres componentes principales. El primero, la conciencia, se refiere al momento en que el individuo reconoce una situación y actúa en consecuencia. El segundo componente es la capacitación, caracterizada por ser un proceso formal orientado a enseñar habilidades específicas. Finalmente, el tercer componente es la educación, que proporciona conocimientos y habilidades bajo un marco teórico integral (Corradini, 2020).

Generar conciencia de ciberseguridad en las juntas directivas implica el reconocimiento de su papel y la comprensión de las implicaciones e impactos de sus decisiones dentro de la organización. Para fortalecer esta conciencia, se debe promover un lenguaje común (Corradini, 2020).

Paso 3. Sensibilizar a los miembros de la junta directiva sobre amenazas cibernéticas y sus consecuencias

La sensibilización en ciberseguridad dirigida a miembros de juntas directivas es relevante, ya que les permitirá mantenerse actualizados y atentos en el cambiante entorno digital. Tal como menciona el SANS Institute (2023) en su publicación *2023 Security Awareness Report,* para alcanzar una madurez en los programas de sensibilización es necesario adoptar un enfoque menos técnico y más orientado a la gestión del riesgo humano. Esto ayudará a que los líderes cambien su percepción sobre la necesidad de contar con una estrategia sólida de ciberseguridad, reforzando su rol y responsabilidad durante los escenarios de respuesta ante incidentes en situaciones de crisis cibernética que pongan en riesgo a la organización.

En este mismo sentido, el programa de sensibilización puede incluir la generación de indicadores que deben ser comunicados a los miembros de la junta directiva para evidenciar el avance en el fortalecimiento de la resiliencia cibernética o para identificar acciones de mejora que deben ser reforzadas.

Se espera que los directivos estén alerta frente a las amenazas cibernéticas a las que pueden estar expuestos, considerando su posición en la organización, así como las consecuencias e impactos que la materialización de un evento cibernético podría acarrear, tales como la indisponibilidad operativa, pérdidas financieras, sanciones legales, pérdida de reputación o incluso acusaciones penales contra los miembros de la junta directiva (Fortinet, 2024).

Conocimiento

El intercambio de conocimiento y el compartir lecciones aprendidas contribuyen a la mejora de la concientización en ciberseguridad (Willie, 2023).

En este sentido, la formación en ciberseguridad debe ser vista como una inversión y no como un costo (Corradini, 2020). Estos programas deben estar diseñados en concordancia con los valores de la organización y orientados al desarrollo de habilidades. Así, el elemento conocimiento en una cultura de ciberseguridad promueve la eficiencia, la innovación y la prosperidad económica en las organizaciones (Da Veiga, 2016).

El incremento de riesgos y amenazas cibernéticas ha llevado a que el conocimiento se convierta en una habilidad esencial, integrada a un comportamiento cibernético de acción inconsciente (Uchendu et al., 2021).

Paso 4. Definir un plan de capacitación en ciberseguridad que contemple sus bases, riesgos y amenazas cibernéticas y las consecuencias para la organización

La planificación de la capacitación debe considerar el contexto específico de cada organización. De acuerdo con Corradini (2020), "los objetivos, etapas, herramientas y técnicas deben planificarse y coordinarse para producir los resultados del aprendizaje que la organización desea lograr". El método de capacitación puede variar según la necesidad y la forma en que se pretenda su implementación (tabla 4).

Como resultado de la capacitación, se espera lograr una mejora en el comportamiento, las actitudes, el cumplimiento, la comunicación, las normas y las responsabilidades en torno a la ciberseguridad.

Tabla 4. *Métodos de capacitación*

Método	Medio	Uso
En línea	Correos electrónicos	Pueden ser usados para difundir nuevos materiales de capacitación, como videos, juegos, hojas de consejos, historias y preguntas frecuentes.
	Videos	Pueden utilizarse con fines de formación, incluyendo charlas de expertos en ciberseguridad (internos o externos).
	Juegos	Facilitan el compromiso, la participación y la apertura al conocimiento.
	Seminarios web	Participación de expertos internos o externos de forma interactiva y rentable para transmitir mensajes de ciberseguridad.
	Cursos de formación en línea	Pueden diseñarse como cursos generales o específicos o por grupo objetivo.
	Intranet	Permite la comunicación con los empleados para entregar material de ciberseguridad.
	Redes sociales	Pueden comunicarse buenas prácticas de ciberseguridad, alertar sobre amenazas específicas y compartir recursos útiles. Los empleados deben seguir las cuentas de la organización.

Método	Medio	Uso
Fuera de línea	Ejecutar escenarios, ensayos, *sandboxes* y ejercicios de juegos de guerra.	Aumenta la preparación para eventos cibernéticos; identifica riesgos; crea comportamientos/respuestas que sean producidas propiamente por el personal.
	Historias	Pueden presentar una respuesta a una amenaza actual, qué medidas tomó el empleado y cuál fue el resultado. Puede estar impresa en folletos o carteleras, o en un video durante una formación en línea. Puede incluir consejos y preguntas.
	Ofrecer incentivos	Puede realizar competencias y brindar productos de la organización a quien haya tenido un mejor desempeño. Estas actividades están ligadas al comportamiento de los individuos.
	Realizar ataques simulados	Pueden incluir ataques en línea con correos electrónicos falsos de *phishing*. Puede incluir llamadas telefónicas falsas a los integrantes de la junta directiva, con el objetivo de probar procesos y procedimientos correctos. Puede realizar simulaciones de sala de crisis para evaluar el desempeño y actuación de los directivos.
Híbridos	Capacitaciones	Reuniones grupales donde los individuos pueden probar sus habilidades, cometer errores y hacer preguntas en un entorno seguro.
	Folletos / carteles	Pueden incluir consejos, preguntas frecuentes, historias cortas y datos de contacto con el equipo de ciberseguridad.
	Talleres	Entorno interactivo para que las personas reciban capacitación, garantizando un entorno positivo para que se sientan seguros al cometer errores o hacer preguntas.
	Eventos	Se centran en la ciberseguridad en general, amenazas específicas y herramientas contra el cibercrimen.
	Conferencias	Las conferencias permiten obtener una comprensión más amplia y actualizada de las tendencias en ciberseguridad.

Fuente: Elaboración propia con base en ENISA (2017).

Comportamientos

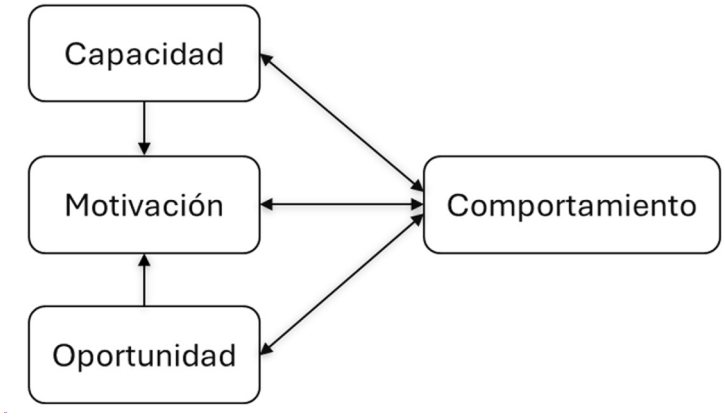
El comportamiento y las actitudes frente a la ciberseguridad por parte de los empleados de una organización están influenciados por la forma en que han adoptado e interiorizado las creencias y valores (González, 2023).

Otros factores, como la capacitación continua, la transmisión de información, ideas y valores, también contribuyen a la formación del comportamiento de cultura de ciberseguridad. Además, fortalecen el empoderamiento de las personas y el desarrollo de capacidades sociológicas y psicológicas, especialmente en contextos que involucran procesos tecnológicos y de ciberseguridad (Álvarez & Urrego, 2019).

Las juntas directivas deben desarrollar estrategias en conjunto con los líderes de proceso para motivar, premiar o, si es necesario, sancionar a los individuos de acuerdo con su comportamiento, ya que este puede fortalecer o debilitar la postura de ciberseguridad de la organización (Hayden, 2016).

Un comportamiento es el resultado de tres variables que todo individuo posee: la habilidad o capacidad de realizar una acción, la motivación que impulsa a llevarla a cabo y la oportunidad de ejecutarla (ENISA, 2021; Michie et al., 2011) (figura 5). Llevando esto al contexto de la cultura de ciberseguridad, puede considerarse el ejemplo de la recepción de un correo de *phishing* por parte de un miembro de la junta directiva, quien debe tener la capacidad de identificar un correo malicioso, la oportunidad de decidir abrirlo o reportarlo, y la motivación para actuar de forma segura.

Figura 5. *Modelo COM-B para entender el comportamiento.*



Fuente: Adaptado de Michie et al. (2011)

A continuación, se indica el paso que permite desarrollar el elemento Comportamiento en los miembros de la junta directiva.

Paso 5. Evaluar el comportamiento en ciberseguridad de los miembros de la junta directiva

Una de las formas de evaluar el comportamiento de los individuos en cuanto a ciberseguridad es a través de ejercicios de ingeniería social, como pruebas de Rocha y Ekstedt (2012), la verificación del uso de cuentas corporativas para actividades personales como redes sociales, o la identificación de prácticas como el escritorio limpio, entre otras. Las acciones que los empleados adopten ante

actividades reales o simuladas que impliquen algún nivel de riesgo permiten identificar el impacto directo o indirecto en la cultura cibernética (ENISA, 2021).

Valores

Desde la perspectiva de ENISA (2017), la evolución de una cultura organizacional comienza con la modificación de sus valores fundamentales, impulsando así la adopción de nuevos comportamientos. Las juntas directivas son quienes establecen el camino para los valores y objetivos de la organización.

Cano (2021) señala que los valores conscientes determinan el comportamiento y la manera en que se realizan las actividades en una organización, estando intrínsecamente ligados a las conductas y conocimientos previos que definen su historia.

En este sentido, los valores representan teorías oficialmente documentadas que no siempre reflejan la realidad de los valores conscientes o inconscientes. Por tanto, la construcción de valores verdaderos debe basarse en una descripción cualitativa sustentada en observaciones oficiales (Schlienger & Teufel, 2005).

De acuerdo con Schein (2017), el conocimiento adquirido de forma colectiva representa las creencias y valores de un individuo, fomentando la cooperación entre sus integrantes y moderando sus actitudes y comportamientos.

Paso 6. Incluir la ciberseguridad como un valor corporativo

Incorporar la ciberseguridad como un valor corporativo orienta a la organización hacia un enfoque proactivo en la protección de sus activos digitales. Según Hayden (2016), la cultura de ciberseguridad debe diseñarse en armonía con los valores y la cultura preexistente de la organización.

Esto implica que las políticas y prácticas de seguridad deben estar alineadas con la identidad corporativa, de modo que sean percibidas no solo como una obligación, sino como una extensión natural de los principios y objetivos fundamentales de la empresa.

Cuando la junta directiva adopta la ciberseguridad como un valor corporativo y lo proyecta hacia toda la organización en un modelo *top-down,* se genera en los colaboradores un sentido de responsabilidad y compromiso con la protección de la información, fortaleciendo así la resiliencia corporativa frente a posibles amenazas.

Normas

Integrar las normativas que regulan el manejo de la información dentro de la cultura de ciberseguridad se considera una finalidad de aplicabilidad no solo en las organizaciones, sino también en las personas (Valencia-Arias et al., 2020).

Por otro lado, Cano (2016) señala que mantener una cultura organizacional implica un cambio en cada individuo, influenciado por el marco normativo de la organización. Las actuaciones de un individuo impactan tanto a nivel interno como externo, ya que sus comportamientos y decisiones pueden afectar la percepción y las prácticas de ciberseguridad dentro de la organización, así como su imagen ante los grupos de interés. En este contexto, el impacto no solo refuerza la cultura de ciberseguridad interna, sino que también marca una tendencia en su entorno, promoviendo estándares y expectativas similares en otras organizaciones y en la industria en general.

Paso 7. Alinear a la organización en el cumplimiento de normativas, estándares o buenas prácticas en ciberseguridad

Una de las responsabilidades de la junta directiva es liderar la implementación de la ciberseguridad en toda la organización. Esto implica alinearse con estándares y buenas prácticas que proporcionen una visión holística de la seguridad empresarial, incluyendo la ciberseguridad, y garantizar el cumplimiento de las regulaciones y normativas locales aplicables al sector.

Además, la adopción de normas, estándares y buenas prácticas permite desarrollar un modelo de medición que ayuda a la organización a identificar su nivel de madurez y las oportunidades de mejora. Uno de los marcos más utilizados a nivel global es el National Institute of Standards and Technology (NIST), que en su versión más reciente (NIST 2.0) incorpora la función de *Gobernanza,* enfocada en identificar y gestionar los riesgos cibernéticos como parte integral de los riesgos empresariales (NIST, 2023).

Síntesis

Al llegar a este punto, se ha identificado que la adopción de una cultura de ciberseguridad en las juntas directivas implica el desarrollo de los pasos descritos en los apartados anteriores. Estos pasos, en conjunto, permitirán a la organización trazar un objetivo claro en el horizonte, en el cual sus directivos adquieran conciencia sobre la importancia de contar con entornos ciberseguros, dada la naturaleza de las amenazas del mundo moderno, para las cuales deben estar preparados y responder adecuadamente cuando sea necesario, favoreciendo la continuidad y la resiliencia corporativa.

La tabla 5 resume los elementos orientadores y sus pasos para construir una cultura de ciberseguridad a nivel directivo.

Tabla 5. *Pasos para adoptar una cultura de ciberseguridad en juntas directivas*

Elemento	Pasos
Estrategia	Paso 1. Medir el nivel de madurez en cultura de ciberseguridad de la junta directiva.
	Paso 2. Designar los recursos necesarios para la gestión de la ciberseguridad.
Concientización	Paso 3. Sensibilizar a los miembros de la junta directiva sobre amenazas cibernéticas y sus consecuencias.
Conocimiento	Paso 4. Definir un plan de capacitación en ciberseguridad que contemple sus bases, riesgos y amenazas cibernéticas y las consecuencias para la organización.
Comportamientos	Paso 5. Evaluar el comportamiento en ciberseguridad de los miembros de la junta directiva.
Valores	Paso 6. Incluir la ciberseguridad como un valor corporativo.
Normas	Paso 7. Alinear a la organización en el cumplimiento de normativas, estándares o buenas prácticas en ciberseguridad.

Fuente: Elaboración propia.

Preguntas de reflexión

Realizar una revisión periódica de la cultura de ciberseguridad en las juntas directivas permite identificar los aspectos de mejora y evaluar los cambios desde su adopción. ENISA también sugiere que esta cultura debe medirse periódicamente para garantizar su éxito a lo largo del tiempo.

De acuerdo con Cano (2023), "el 51 % de las organizaciones afirma que los altos directivos se han enfrentado a multas, penas de cárcel, pérdida del puesto o pérdida del empleo tras un ciberataque". Ante este dato, resulta pertinente preguntarse: ¿Qué hace que los miembros de las juntas directivas no muestren un mayor interés en la ciberseguridad?

La junta directiva debe también reflexionar sobre cómo se puede medir su preparación frente a las amenazas cibernéticas y si la organización cuenta con los mecanismos adecuados para enfrentarlas. Es importante que el responsable de ciberseguridad en la organización informe periódicamente a la junta directiva mediante reportes que incluyan estadísticas sobre pérdidas económicas, daños reputacionales o afectaciones operativas (Clinton et al., 2023).

Asimismo, surge el cuestionamiento: ¿Debería la junta directiva contar entre sus integrantes con un experto en ciberseguridad? Esto no implica que dicha persona asuma individualmente la responsabilidad o tome decisiones de manera

aislada ante la materialización de un riesgo o incidente cibernético; más bien, su experticia contribuiría a aumentar el nivel de comprensión de la ciberseguridad dentro de la junta directiva, tal como señalan Clinton et al. (2023).

Conclusiones

Dentro de esta investigación se concluye que la ciberseguridad es contemplada por los directivos, aunque no con la relevancia y frecuencia necesarias. Un punto de partida para la apropiación de este tema es incluir en la agenda de las juntas directivas un espacio específico para discutir asuntos de ciberseguridad, lo cual permitiría abrir el debate sobre ataques dirigidos a la organización o al sector al que pertenece. Surge así la necesidad de preguntarse cuál es el impacto y las consecuencias de la materialización de riesgos.

La perspectiva hacia los integrantes de las juntas directivas es que su postura frente a los riesgos de ciberseguridad sea estratégica. No obstante, esta visión puede verse debilitada por la falta de habilidades, conocimientos y métricas claras, lo que dificulta el análisis y la asignación adecuada de recursos destinados a la ciberseguridad.

Los elementos seleccionados en el desarrollo de esta guía apoyan el fomento de una cultura de ciberseguridad a nivel de juntas directivas. Estos elementos buscan influir en el comportamiento a partir del conocimiento adquirido, promoviendo una toma de decisiones consciente sobre el impacto y la relevancia de la ciberseguridad para la organización. Esta adopción está vinculada tanto a la cultura organizacional interna como a las buenas prácticas observadas desde una perspectiva externa.

La investigación resalta que la concientización y la capacitación en ciberseguridad son fundamentales para las juntas directivas. La falta de conocimiento y preparación puede llevar a decisiones mal informadas que pongan en riesgo la seguridad de la organización. La implementación de programas de sensibilización y formación continua resulta crucial para que los directivos comprendan los riesgos cibernéticos y sus posibles consecuencias.

Las juntas directivas deben asumir un rol estratégico en la gestión de la ciberseguridad. Esto incluye la asignación adecuada de recursos, la creación de comités específicos y la integración de la ciberseguridad en la estrategia corporativa. La investigación destaca que la ciberseguridad no debe ser vista como una responsabilidad exclusiva del departamento de TI, sino como una prioridad organizacional que requiere el compromiso de todos los niveles directivos.

La adopción de una cultura de ciberseguridad en las juntas directivas implica un cambio en la percepción y comportamiento de sus miembros. Es esencial que estos líderes comprendan la importancia de la ciberseguridad y promuevan prácticas seguras dentro de la organización. La investigación propone una guía con elementos orientadores —estrategia, concientización, conocimiento, comportamientos, valores y normas— que puede apoyar a las juntas directivas en el establecimiento de una cultura de ciberseguridad sólida y resiliente.

Recomendaciones

Desarrollo de programas de capacitación personalizados: Crear programas de capacitación en ciberseguridad adaptados a las necesidades específicas de las juntas directivas. Estos programas deben incluir simulaciones de incidentes cibernéticos, estudios de caso y talleres prácticos que permitan a los directivos experimentar y gestionar situaciones reales de ciberseguridad.

Investigación sobre la eficacia de las políticas de ciberseguridad: Realizar estudios longitudinales que evalúen la eficacia de las políticas y estrategias de ciberseguridad implementadas en las organizaciones. Esta información permitirá identificar buenas prácticas y áreas de mejora, proporcionando datos relevantes para la toma de decisiones informadas.

Integración de la ciberseguridad en la cultura organizacional: Investigar métodos para integrar de manera efectiva la ciberseguridad dentro de la cultura organizacional, incluyendo el desarrollo de marcos teóricos y prácticos que faciliten la adopción de comportamientos seguros y fomenten un entorno de trabajo que valore y priorice la ciberseguridad.

Evaluación de la madurez en ciberseguridad: Desarrollar y aplicar modelos de evaluación de madurez en ciberseguridad que permitan medir el progreso organizacional y establecer metas claras. Estos modelos deben considerar factores como la concientización, la capacitación, la asignación de recursos y la implementación de tecnologías de seguridad.

Colaboración intersectorial: Fomentar la colaboración entre sectores y organizaciones para compartir conocimientos y experiencias en ciberseguridad. La creación de redes y alianzas estratégicas fortalecerá las capacidades de ciberseguridad a nivel nacional e internacional, promoviendo un enfoque más cohesivo y coordinado frente a las amenazas cibernéticas.

Referencias

Advice Group LATAM. (2023, 9 de agosto). *Estadísticas de ciberseguridad en Centroamérica y Colombia.* https://tinyurl.com/2yu2mkpr

AlHogail, A., & Mirza, A. (2014a). A proposal of an organizational information security culture framework. En *Proceedings of International Conference on Information, Communication Technology and System (ICTS) 2014* (pp. 243-250). https://doi.org/10.1109/ICTS.2014.7010591

AlHogail, A., & Mirza, A. (2014b). Information security culture: A definition and a literature review. *2014 World Congress on Computer Applications and Information Systems (WCCAIS),* 1-7. https://doi.org/10.1109/WCCAIS.2014.6916579

AL-sartawi, A. (2020). Information technology governance and cybersecurity at the board level. *International Journal of Critical Infrastructures, 16*(2), 150-161. https://doi.org/10.1504/IJCIS.2020.10029173

Álvarez Dionisi, L. E., & Urrego Baquero, N. (2019, 15 de marzo). Implementing a cybersecurity culture. *ISACA.* https://tinyurl.com/2ch7q7j7

Azuero Zúñiga, F., Cuéllar Boada, F. H., Moya Suárez, J., Serna Hernández, S., Romero Ortiz, L. E., & González Couture, G. A. (2020). *Juntas directivas, eje del gobierno corporativo* (1.ª ed.). Ediciones Uniandes.

Barrero, V., & Bou, O. (2020). *Estado de preparación en ciberseguridad del sector eléctrico en América Latina.* BID. https://doi.org/10.18235/0002344

Bertalanffy, L. von. (1989). *Teoría general de los sistemas.* Fondo de Cultura Económica.

Cano, J. (2016, octubre). Modelo de madurez de cultura organizacional de seguridad de la información. Una visión desde el pensamiento sistémico-cibernético. En *XIV Reunión Española sobre Criptología y Seguridad de la Información* (Vol. 1, pp. 24-29). https://tinyurl.com/24nas3rx

Cano, J. (2021, 16 de junio). *Cultura organizacional de seguridad de la información. Una perspectiva sistémica de articulación de sistemas humanos, culturales y sociales.* ISACA. https://tinyurl.com/4hkbjv63

Cano, J. (2023). *Ciberseguridad empresarial: Reflexiones y retos para los ejecutivos del siglo XXI* (2.ª ed.). Ediciones de la U.

Clinton, L., Marx, A., Swafford, K., & Sandlin, D. (2023). *Director's handbook on cyberrisk oversight* (National Association of Corporate Directors [NACD], Ed.). https://tinyurl.com/2xemty5x

Consejo Nacional de Política Económica y Social (CONPES) 3701. (2011, 14 de julio). *Lineamientos de política para ciberseguridad y ciberdefensa.* Departamento Nacional de Planeación. https://tinyurl.com/mrb3nfdt

Consejo Nacional de Política Económica y Social (CONPES) 3995. (2020, 1 de julio). *Política Nacional de Confianza y Seguridad Digital.* Departamento Nacional de Planeación. https://tinyurl.com/4xxep7f6

Corradini, I. (2020). *Building a cybersecurity culture in organizations: How to bridge the gap between people and digital technology.* Springer International Publishing. https://doi.org/10.1007/978-3-030-43999-6

Cyber Citadel. (2023). *Cyber security guide for board directors.* https://tinyurl.com/b368dfwd

Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. *2016 SAI Computing Conference (SAI),* 1006-1015. https://doi.org/10.1109/SAI.2016.7556102

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29*(2), 196-207. https://doi.org/10.1016/j.cose.2009.09.002

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review, 31*(2), 243-256. https://doi.org/10.1016/j.clsr.2015.01.005

Dornheim, P., & Zarnekow, R. (2023). Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information & Computer Security* (publicación anticipada). https://doi.org/10.1108/ICS-07-2023-0116

European Union Agency for Cybersecurity (ENISA). (2017, noviembre). *Cyber security culture in organisations* [informe/estudio]. https://tinyurl.com/2a3bae6m

European Union Agency for Cybersecurity (ENISA). (2021). *Review of behavioural sciences research in the field of cybersecurity: Technical annex: Evidence reviews.* Publications Office. https://data.europa.eu/doi/10.2824/717888

Fortinet. (2024). *2024 Cybersecurity Skills Gap*. https://tinyurl.com/4u5auzhs

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security, 121*, 102840. https://doi.org/10.1016/j.cose.2022.102840

Giraldo Ríos, L. A. (2024). Definición e impacto en la transformación digital y la ciberseguridad. En M. E. Realpe Díaz, & A. M. González González (Eds.), *Tecnologías disruptivas, logística y seguridad y defensa nacional en el ciberespacio* (pp. 15-46). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602700.01

Goicoechea de Jorge, M. (2004). *El lector en el ciberespacio: Una etnografía literaria de la cibercultura* [tesis doctoral, Universidad Complutense de Madrid]. https://eprints.ucm.es/id/eprint/32979/1/T27652.pdf

González Sánchez, D. A. (2023). *Modelo de madurez de cultura organizacional de ciberseguridad para el sector financiero basado en buenas prácticas* [tesis de maestría, Tecnológico de Antioquia, Colombia]. https://dspace.tdea.edu.co/handle/tdea/3927

González, J. A., Amozurrutia, J. A., & Maass, M. (2007). *Cibercultur@ e iniciación en la investigación.* UNAM.

Hayden, L. (2016). *People-centric security: Transforming your enterprise security culture.* McGraw-Hill Education.

Hernández Sampieri, R., & Fernández Collado, C. (2014). *Metodología de la investigación* (P. Baptista Lucio, Ed.; 6.ª ed.). McGraw-Hill Education.

Hofstede, G. (1980). Motivation, leadership, and organization: Do American theories apply abroad? *Organizational Dynamics,* 9(1). https://doi.org/10.1016/0090-2616(80)90013-3

Hogail, A. A. (2015). Cultivating and assessing an organizational information security culture: An empirical study. *International Journal of Security and Its Applications, 9*(7), 163-178. https://doi.org/10.14257/ijsia.2015.9.7.15

IBM Security. (2023). *Cost of a data breach report.* IBM. https://www.ibm.com/reports/data-breach

Institute of Internal Auditors (IIA). (2021). *OnRisk: A guide to understanding, aligning, and optimizing risk.* IIA. https://iiabelgium.org/wp-content/uploads/2020/11/OnRisk-2021-Report.pdf

Maurer, T., Taylor, K., & Grossman, T. (2020, diciembre). *Capacity-Building Tool Box for Cybersecurity and Financial Organizations.* https://tinyurl.com/3h6pyw2x

Michie, S., van Stralen, M., & West, R. (2011). The Behaviour Change Wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science: IS, 6*, 42. https://doi.org/10.1186/1748-5908-6-42

Milică, L., & Pearlson, K. (2023, 2 de mayo). Boards are having the wrong conversations about cybersecurity. *Harvard Business Review.* https://tinyurl.com/2g59rd66

National Institute of Standards and Technology (NIST). (2023). *The NIST Cybersecurity Framework 2.0* (NIST CSWP 29 ipd). https://tinyurl.com/mrymfbf5

Nodehi, S., Huygh, T., & Bollen, L. (2024). Six board roles for information security governance. En *Proceedings of the 26th International Conference on Enterprise Information Systems* (pp. 713-720). https://doi.org/10.5220/0012695900003690

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems, 12*(2). https://doi.org/10.1145/3424282

Organización de Estados Americanos (OEA). (2004, 8 de junio). *Adopción de una estrategia interamericana integral de seguridad cibernética.* https://tinyurl.com/5n87uz48

Organización de Estados Americanos (OEA). (2018). *Critical infrastructure protection in Latin America and the Caribbean 2018.* https://www.oas.org/es/sms/cicte/cipreport.pdf

Organización de Estados Americanos (OEA). (2019, 27 de septiembre). *Manual de supervisión de riesgos cibernéticos para juntas corporativas.* https://tinyurl.com/z4vaxhfh

Pearlson, K., Sposito, S., Arbisman, M., & Schwartz, J. A. (2021, 30 de septiembre). How Yahoo built a culture of cybersecurity. *Harvard Business Review.* https://hbr.org/2021/09/how-yahoo-built-a-culture-of-cybersecurity

PricewaterhouseCoopers. (2020). *Informe del estado de cultura de ciberseguridad en el entorno empresarial.* https://tinyurl.com/3ntfz28x

Rocha Flores, W., & Ekstedt, M. (2012, 15 de diciembre). A model for investigating organizational impact on information security behavior. En *Proceedings of the 7th International Conference on Availability, Reliability and Security* (pp. 660-667).

Ruiz Olabuénaga, J. I. (2012). *Metodología de la investigación cualitativa* (5.ª ed.). Universidad de Deusto.

SANS Institute. (2023). *SANS 2023 Security Awareness Report.* https://tinyurl.com/3zjbnux8

Schein, E. H. (2017). *Organizational culture and leadership* (5.ª ed.). John Wiley & Sons.

Schlienger, T., & Teufel, S. (2005). Analyzing information security culture: Increased trust by an appropriate information security culture. En *Proceedings of the 14th International Workshop on Database and Expert Systems Applications* (pp. 405-409). https://doi.org/10.1109/DEXA.2003.1232055

Schneider, B., Asprion, P. M., Androvicsova, S., & Azan, W. (2020). *A practical guideline for developing a managerial information security awareness program.*

Schwab, K. (2016). *La cuarta revolución industrial.* Marcial Pons.

Steele, G. (2024). *The hidden costs of downtime,* 26.

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cybersecurity culture: Current practices and future needs. *Computers & Security, 109,* 102387. https://doi.org/10.1016/j.cose.2021.102387

Valencia-Arias, A., Giraldo, M. C. B., Acevedo-Correa, Y., Garcés-Giraldo, L. F., Quiroz-Fabra, J., Benjumea-Arias, M. L., & Patiño-Vanegas, J. C. (2020). Tendencias investigativas en educación en ciberseguridad: Un estudio bibliométrico. *Revista Latinoamericana de Investigación en Seguridad Informática, 8*(3), 225-239. https://tinyurl.com/2bwj7moc

Vasilachis de Gialdino, I. (2006). *Estrategias de investigación cualitativa* (1.ª ed.). Editorial Gedisa.

Verizon Business. (2023). *Data Breach Investigation Report 2023 (DBIR).* https://tinyurl.com/4zz7z3a5

Willie, M. (2023). *The role of organizational culture in cybersecurity: Building a security-first culture*. SSRN. https://dx.doi.org/10.2139/ssrn.4564291

World Economic Forum. (2022). *The Global Risks Report 2022* (Informe 17). https://tinyurl.com/yc5w4wy6

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005