Centro UC
Gobierno Corporativo

DIÁLOGOS DE GOBIERNO CORPORATIVO

CGC UC

CICLO DE ENCUENTROS DE DIRECTORES CGC UC - DELOITTE 2023

CIBERSEGURIDAD: LOS PRINCIPALES FOCOS DE ATENCIÓN DEL DIRECTORIO

Sebastián Melero

Carla Meza

Ciclo de diálogos 2023

con la colaboración de Deloitte.

El presente documento tiene su origen en las conversaciones sostenidas por los participantes del CICLO DE ENCUENTROS DE DIRECTORES 2023 CGC UC - DELOITTE, realizado los días 11 de abril y 9 de mayo 2023 y organizado por el Centro de Gobierno Corporativo de la Pontificia Universidad Católica de Chile, CGC UC, y DELOITTE. La presentación ha sido editada para efectos de la publicación de este documento sin necesariamente adscribir una opinión específica a un participante específico. El presente documento ha sido desarrollado por el investigador asociado Sebastián Melero y editado por la investigadora asociada Carla Meza. Todo posible error en la transcripción es de exclusiva responsabilidad de CGC UC.

I. INTRODUCCIÓN

El aumento en el uso de internet, auge de redes sociales, desarrollo continuo de la inteligencia artificial, entre otros factores, revelan que estamos experimentando una verdadera revolución digital. Este fenómeno ha afectado a personas, instituciones y empresas en todo el mundo.

En las compañías, donde varios de los activos han tendido a transformarse en digitales se ha producido la llamada "digitalización" del riesgo corporativo. Como plantea el "*Manual de Supervisión de Riesgos Cibernéticos para Juntas Corporativas*" de la Organización de los Estados Americanos (OEA)[1], uno de los mayores riesgos a los que se ven expuestas las empresas son los llamados "ciberataques". Estos ataques no solo pueden provocar la pérdida de propiedad intelectual y planes comerciales, así como la destrucción o alteración de datos, sino que también pueden socavar la confianza del público en la empresa con un daño reputacional enorme.

En este escenario, la ciberseguridad, entendida como el conjunto de prácticas y medidas diseñadas para proteger los sistemas y datos de amenazas y ataques cibernéticos, adquiere especial relevancia.

El Centro de Gobierno Corporativo de la de la Pontificia Universidad Católica de Chile ("CGC UC") es un referente de buenas prácticas de Gobierno Corporativo, motivado no sólo por la excelencia académica, sino por el propósito de ser un punto de encuentro en la discusión de temas de gobierno corporativo de interés para los directores y para el debate a nivel país. En este contexto, con el objetivo de reunir a directores y expertos en el área para reflexionar sobre este nuevo desafío empresarial y posibles acciones que se podrían tomar a nivel de directorio para enfrentar los riesgos cibernéticos, el CGC UC y Deloitte organizaron un ciclo de encuentros para reflexionar sobre ciberseguridad.

Estos encuentros se llevaron a cabo los días 11 de abril y 9 de mayo, titulados "*Ciberseguridad desde el directorio y la gestión de riesgos*", y "*Ciberseguridad, los próximos desafíos*".

El primer encuentro fue moderado por Matías Zegers, Presidente Ejecutivo del CGC UC, y contó con la participación de Nicolás Corrado, socio líder de Ciberseguridad de Deloitte y Tina Rosenfeld, directora de empresas, como panelistas. El segundo encuentro, tuvo por moderadora a Tatiana Molina, directora de Corporate Governance Deloitte, y como panelistas a María Luisa Acuña, socia de ciberseguridad de Deloitte y Claudio Muñoz, director de empresas. Ambos encuentros contaron con la participación de directoras y directores de empresas, asesores legales y de estrategia y otros participantes de gobierno corporativo que conversaron activamente con los panelistas y que compartieron inquietudes y buenas prácticas.

A continuación, se resumen los principales puntos abordados por el panel y los directores invitados en cada uno de los encuentros.

[1] El documento puede consultarse de manera digital en: https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf [fecha de acceso: 30 de mayo de 2023].

II. CIBERSEGURIDAD DESDE EL DIRECTORIO Y LA GESTIÓN DE RIESGOS.

2.1. La digitalización, seguridad y el desafío empresarial en un mundo conectado.

No es ningún misterio que el mundo avanza rápidamente hacia la digitalización de sistemas y empresas, proceso que se aceleró durante la pandemia. En la actualidad, la digitalización se ha convertido en una poderosa herramienta para impulsar el éxito de las empresas. Los líderes empresariales tienen un gran desafío de comprender las ventajas que ofrece la digitalización en un ecosistema altamente competitivo. Entre otros, la digitalización facilita la recopilación y análisis de datos en tiempo real, lo que les permite tomar decisiones más informadas y estratégicas. La digitalización ofrece nuevas oportunidades de comunicación y colaboración tanto interna como externa, permitiendo una mayor agilidad en la toma de decisiones y una mejora en la atención al cliente. Asimismo, la digitalización fomenta la innovación y la creatividad al facilitar la experimentación con nuevas tecnologías y modelos de negocio.

Sin perjuicio de los grandes beneficios de la digitalización, hoy todas las empresas conectadas a internet enfrentan distintos desafíos en esta materia, uno de ellos, los riesgos de seguridad en el mundo digital. En este sentido, se hace necesario cambiar la percepción de que la seguridad digital es algo ajeno a ciertas organizaciones y reconocer que es una parte integral del negocio que debe ser gestionada por las empresas de forma transversal, tengan mayor o menor exposición al mundo digital dado que es un riesgo que tiene una naturaleza diferente, donde hay estructuras delictivas organizadas destinadas a explotar las debilidades de las compañías.

2.2. Los directores cumplen un rol clave en la estrategia de riesgos digitales.

En el contexto de la digitalización, los directores se enfrentan a una serie de desafíos que requieren una atención estratégica y una comprensión profunda de las implicaciones y los riesgos de esta transformación tecnológica, que converse adecuadamente con su deber de cuidado. Sin embargo, gestionar este tipo de temas es difícil para directores que usualmente no son expertos en la materia y que no necesariamente son “nativos digitales”.

Las respuestas ante el desafío son múltiples, ante ello, los directores presentes reflexionaron sobre la importancia de efectuar un correcto diagnóstico del conocimiento y de las capacidades, de la capacitación y de abordar el desafío con una mentalidad de cambio, aprendiendo de experiencias comparadas que pueden resultar útiles a la hora de definir estrategias.

Hay distintas formas de enfrentarse al desafío, lo que variará según las circunstancias de cada compañía en particular. Una opción que se ha implementado por ejemplo en Estados Unidos, especialmente en casos en que el negocio no es digital, es la creación de comités de seguridad que efectúen reportes al directorio. Otra opción es incluir talento digital directamente en el directorio; Aunque es improbable que todos los directores tengan un alto nivel de conocimiento en seguridad digital, es bueno que, de justificarse las circunstancias, al menos exista uno con tal conocimiento para que pueda pronunciarse respecto a dichos reportes.

Además, los reguladores han elevado el estándar de responsabilidad de los directores, no limitándose solo al ámbito de tecnología de la información (así por ejemplo, la Comisión de Valores y Bolsa de Estados Unidos o Securities and Exchange Commission). Esto sugiere

que los directores deben asumir una mayor responsabilidad en la gestión de la seguridad digital en las organizaciones.

2.3. La cultura empresarial es clave para la prevención del riesgo.

Por la envergadura del riesgo de ciberseguridad, es de aquellos que permean a toda la organización, por lo que se reflexionó sobre la necesidad de que exista una cultura de seguridad frente al riesgo que abarque a toda la compañía. Esta cultura no puede ser impuesta “desde el directorio hacia abajo”, sino que es necesario generar una conciencia personal en cada miembro de la empresa, aparejada a una responsabilidad individual.

Es importante recalcar que la gestión de riesgos cibernéticos en una empresa no debe ser solo un tema de tecnologías de información, sino que debe existir un vínculo integral con los demás actores de la compañía y preocupación real al respecto. Es crucial que exista colaboración entre distintos agentes para definir cuáles son los activos que se quieren proteger, los riesgos a los que se enfrenta la empresa en materia de ciberseguridad y los recursos con los que se cuenta para enfrentarlos. Con esto en mente, se debe definir una estrategia de seguridad, integrada al mapa de la compañía.

En esta línea, es necesario encontrar un equilibrio entre la estrategia empresarial y la cultura de seguridad, reconociendo que ambas se complementan. La capacidad de integrar una estrategia sólida de ciberseguridad con la cultura organizacional permitirá a las empresas adaptarse y responder de manera eficaz a amenazas en constante cambio.

Una de las formas de poner esto en práctica es que el tema de la ciberseguridad esté presente desde el inicio de cualquier proyecto, y que no sea considerada como una preocupación secundaria o posterior.

Otro punto importante para destacar es que este es un riesgo cuya gestión es altamente preventiva y no reactiva. La aplicación de una sanción en relación con la seguridad digital debe considerarse una mala noticia. Es importante tomar medidas proactivas para evitar posibles sanciones y mitigar los riesgos de seguridad antes de que ocurran problemas.

Finalmente, se conversó sobre la necesidad de entender que nunca se puede lograr una seguridad del 100%. Los ataques cibernéticos se repiten con frecuencia y son cada vez más complejos y elaborados, por lo tanto, la gestión integral de riesgos y la ciberseguridad requieren de una constante vigilancia y adaptación a las nuevas amenazas.

2.4. Acciones en materia de ciberseguridad que puede tomar el directorio.

En materia de ciberseguridad, se conversó sobre diversas acciones que el directorio puede utilizar para fortalecer la protección de la organización, siempre tomando en consideración la realidad de la compañía que se trate y la industria en la que se desarrolla:

(i) Establecer un responsable o un grupo de personas dedicadas a la ciberseguridad, con independencia de criterio y acción, que se encargue de supervisar y gestionar esta área de manera especializada.

(ii) Garantizar que exista una estrategia a nivel de gobierno corporativo respaldando las decisiones y acciones relacionadas con la ciberseguridad. Esto implica establecer políticas y procedimientos claros que respalden las iniciativas de protección.

(iii) Desarrollar una estrategia de protección basada riesgo definido por la organización. En otras palabras, evaluar los riesgos a los que se enfrenta la empresa y diseñar medidas de seguridad adecuadas para mitigarlos.

(iv) Implementar un monitoreo constante para detectar posibles ataques cibernéticos y evaluar correctamente las fuentes de riesgo. Es fundamental asegurarse de contar con sistemas y herramientas adecuadas para identificar las intrusiones y tomar medidas rápidas y efectivas.

Se compartió como mejor práctica el abordar el manejo de dispositivos móviles y la gestión de la información que se realiza a través de ellos, ya que representan una fuente de riesgos significativa para las asociaciones.

(v) Mejorar la respuesta ante incidentes de seguridad. Muchas compañías fallan en este aspecto al no probar y ensayar las respuestas ante situaciones de emergencia. Es importante establecer un plan de respuesta, simular contingencias y garantizar que todos los implicados sepan cómo actuar y reportar adecuadamente los incidentes.

(vi) Enfatizar en el rol del comité de ciberseguridad, definiendo su frecuencia de reuniones y responsabilidades específicas. Esto permite asegurar una supervisión adecuada y una mayor rendición de cuentas en materia de ciberseguridad.

(vii) Fomentar la autoevaluación de la organización, lo cual contribuye a elevar los estándares de seguridad. Se compartió como mejor práctica que un mecanismo útil para evaluar la gestión de riesgo en las empresas es la implementación de cuestionarios de autoevaluación. Estos cuestionarios permiten identificar áreas de mejora y detectar posibles brechas en la gestión de riesgos, brindando una oportunidad para fortalecer controles y medidas de seguridad.

(viii) Es importante que los análisis e indicadores de riesgo estén presentes en los informes y reportes del directorio, proporcionando una visibilidad clara sobre el estado actual de la seguridad de la organización.

(ix) Establecer un plan de capacitación para los directores, incentivando la adquisición de conocimientos en ciberseguridad. Esto puede incluir la participación de expertos que brinden orientación práctica y estrategias aplicables a la realidad de cada director, nivelando el conocimiento en la mesa directiva.

En resumen, el directorio debe tomar medidas proactivas para fortalecer la ciberseguridad de la organización, incluyendo la designación de responsables, la definición de estrategias, el establecimiento de mecanismos de monitoreo y respuesta, el fortalecimiento del comité de ciberseguridad, la promoción de la capacitación y la generación de reportes claros y evaluaciones periódicas.

III. CIBERSEGURIDAD, LOS PRÓXIMOS DESAFÍOS.

3.1. La importancia de la ciberseguridad a nivel de directorio.

El diagnóstico general en la conversación es que la ciberseguridad no es un tema que se aborde con la intensidad necesaria a nivel de directorio. A menudo, este aspecto queda

relegado a áreas intermedias, como de tecnologías de información (TI). Sin embargo, considerando los avances que existen en el área, como la inteligencia artificial, y la gravedad que supone un ataque informático, toda vez que afecta al negocio en sí mismo, es necesario formarse en ciberseguridad y darle mayor relevancia a nivel de directorio.

En el entorno digital, los “firewalls” ya no son suficientes. La estrategia de ciberseguridad debe centrarse en la resiliencia, es decir, en la capacidad de determinar de qué forma se va a reaccionar, hacerlo rápidamente y comunicarse de forma efectiva frente a nuevos ataques.

Hoy es necesario que los directores comprendan la importancia de la ciberseguridad. Esto implica darle prioridad al tema (se recomendó “*nunca estar tranquilos, siempre estar razonablemente inquietos*”), formarse en la materia y adoptar una estrategia basada en la resiliencia basada en los constantes desafíos del mundo digital.

3.2. Desafíos estratégicos de la ciberseguridad.

La ciberseguridad se ha convertido en un riesgo estratégico de gran relevancia para las empresas. Los factores actuales, como la creciente digitalización y la interconexión tecnológica, aumentan los riesgos asociados a ella. Ahora bien, es importante tener presente que la ciberseguridad va más allá de la tecnología. Es una ciencia desafiante que requiere una gestión integral de riesgos, que permee a toda la organización.

El “Manual de Supervisión de Riesgos Cibernéticos” destaca varias consideraciones que son claves al referirse a la ciberseguridad:

(i) La ciberseguridad es un problema de gestión de riesgos que debe abordarse en todos los niveles de la empresa.

(ii) Los riesgos cibernéticos conllevan implicancias legales.

(iii) Es fundamental contar con acceso a la experiencia en ciberseguridad y asegurar que las agencias dispongan de los tiempos necesarios para abordar adecuadamente esta área.

(iv) La discusión sobre la ciberseguridad debe incluir un plan de tratamiento de riesgos que contemple medidas para mitigar, evitar y transferir los riesgos identificados.

(v) Es necesario establecer un marco de gestión de riesgos que cuente con un personal capacitado y presupuesto adecuado para implementar las adecuadas medidas de seguridad.

(vi) Es importante definir el enfoque de gobierno corporativo que se le dará al tema de la ciberseguridad, promover la existencia de una estrategia clara en este ámbito y, para asegurar una supervisión efectiva, requerir un reporte detallado con avances sobre las iniciativas en ciberseguridad.

3.3. Algunos consejos para la gestión del riesgo

La forma en la que las empresas deben gestionar el riesgo cibernético depende de una serie de circunstancias específicas que hacen que una misma solución pueda no ser óptima para dos compañías distintas.

Un consejo útil es partir por definiciones de riesgo, el establecimiento de una estrategia y efectuar un levantamiento de necesidades. La definición del riesgo parte por la designación de un responsable y la formulación del apetito de riesgo y la tolerancia al mismo que cada compañía decide considerando sus circunstancias particulares. Es bueno que estas definiciones se establezcan a través de políticas que puedan ser conocidas por toda la organización.

Una vez determinado el marco de la gestión del riesgo, debe crearse una estrategia de ciberseguridad que evolucione conforme se alcanzan ciertos grados de madurez. La estrategia debe determinar responsables, levantamiento de brechas, planes de tratamiento de brechas y planes de acción. Junto con esta estrategia es fundamental la generación de un plan de capacitación y *awareness* para toda la organización.

Los directores conversaron sobre las dificultades de incorporar cambios en la cultura corporativa, pero la necesidad de efectuarlo de manera consciente y que involucre a todos los estamentos de la compañía.

También se conversó sobre la importancia de generar planes de gestión de crisis, tanto a nivel de incidentes de ciberseguridad mismos como a nivel comunicacional. Tener identificados a los responsables, los planes de resolución y las vocerías ayuda a la resiliencia de la compañía y por lo tanto es fundamental que el directorio la conozca y se involucre cuando los niveles de materialización del riesgo sean altos.

Una vez realizadas las definiciones y habiéndose establecido una estrategia y un plan de incorporación en la cultura corporativa, es tremendamente importante generar un plan de seguimiento de la gestión del riesgo a través de KPIs correctos, que entreguen información clave al directorio sin inundarlo de datos.

En este punto se dialogó sobre la dificultad de los directores de influenciar sobre los KPIs correctos, ya que muchas veces los ejecutivos cuentan con información especializada que puede ser difícil de comprender para directores no especialistas en el tema digital. La discusión se generó respecto de la necesidad de constante capacitación de los directores, de la construcción de una relación y diálogo constante con el responsable del tema, por la mejora continua del seguimiento y la mejora en la elección de KPIs cuando se va conociendo más sobre el tema.

Una vez que se han definido los riesgos, es necesario decidir su tratamiento, el que puede incluir la modificación del riesgo (el nivel de riesgo se reduce mediante la selección de controles de seguridad que llevan el riesgo residual a un nivel aceptable), evitar el riesgo (en el caso de riesgos demasiado altos), aceptar el riesgo (convivir con las posibilidades de materialización, en cuyo caso es bueno que estas decisiones queden documentadas) o transferir el riesgo (sea a través de posibles pólizas de seguros o a través de la contratación de especialistas en temas muy específicos).

3.4. Algunos consejos prácticos de cómo reportar

Es fundamental que la Ciberseguridad sea comunicada adecuadamente, porque es necesaria para la toma de decisiones. Hay un consenso de que es difícil canalizar la información adecuada a los directores, que realmente permita comparar del desempeño y analizar oportunidades de mejora, pues los directores – que no son especialistas en la

materia – tienen dificultad para interpretar la información y para descubrir posibles brechas escondidas en la información entregada.

Por otra parte, los especialistas en materias de seguridad de la información muchas veces utilizan un lenguaje propio que hace difícil aproximarse a los temas, o tienen conocimientos muy robustos que inhiben a los directores a preguntar o profundizar temas.

Por ello, se han recopilados algunos ejemplos prácticos para que los directores soliciten información sobre ciberseguridad en sus organizaciones:

1) La información de gestión de riesgos de ciberseguridad debe ser fácil de leer. Para prevenir los problemas de falta de entendimiento de información compleja, se deben preferir elementos gráficos, visuales, o resúmenes que faciliten información a personas no expertas en la materia. Si la información presentada no es fácil de entender, el director debe solicitar que sea bajada de la manera correcta.

Adicionalmente, el lenguaje que se utiliza debe permitir la aproximación de directores no expertos y no debe inhibir a directores a preguntar porque es un mundo y lenguaje ajeno.

2) La información debe transmitir conocimiento, permitiendo resaltar cambios, patrones, comportamientos, que permitan visibilizar puntos de posibles brechas y puntos de mejora.

3) La información que se debe reportar es aquella que tiene impacto en el negocio, como incidentes, pérdidas, impactos en las transacciones o clientes. Para ello es relevante definir qué información es aquella que tiene impacto y cómo se mide ese impacto.

4) La información debe seleccionarse. Se debe evitar la inundación de información ("*cuanto todo es importante nada es importante*"). No se puede informar todo, se debe refinar aquella información que es realmente útil para los altos ejecutivos o para el directorio para tomar decisiones estratégicas y mitigar riesgos.

IV. CONCLUSIONES.

La digitalización y el aumento en el uso de internet han llevado a una transformación en las empresas. La ciberseguridad se ha vuelto crucial en este escenario, y se requiere que los directores y el directorio de una empresa tomen medidas proactivas para proteger los sistemas y datos de amenazas y ataques cibernéticos que pueden provocar pérdida de datos y dañar la reputación de las empresas.

Hoy la ciberseguridad es un riesgo estratégico que va más allá de la tecnología y debe abordarse en todos los niveles de la empresa. Requiere una gestión integral de riesgos, acceso a la experiencia en ciberseguridad, presupuesto adecuado y un marco de gestión de riesgos bien definido. Esto incluye establecer responsables de ciberseguridad, desarrollar estrategias de protección basadas en los riesgos identificados y mejorar la respuesta ante incidentes de seguridad.

Los directores deben asumir una mayor responsabilidad en la gestión de la seguridad digital en las organizaciones. La creación de comités de seguridad y la capacitación de los directores en ciberseguridad son acciones recomendadas. Además, la colaboración y el intercambio de información entre empresas afectadas por ciberataques o compartir mejores prácticas pueden ser beneficiosos para fortalecer la seguridad en general.

Instancias como esta conversación organizada por el CGC UC y Deloitte son buenas para no sólo reflexionar sobre temas contingentes sino además que los directores logren ser un agente de cambio en sus organizaciones, influenciando el debate público y promoviendo mejores prácticas en el entorno empresarial.

Centro UC
Gobierno Corporativo

www.centrogobiernocorporativo.uc.cl

cgcuc@uc.cl

centro-de-gobierno-corporativo-uc

Rosario Norte 407, Las Condes, Santiago, Chile