LITORALPRESS

Fecha: 14-11-2024
Medio: El Mercurio
Supl. : El Mercurio - Innovacion
Tipo: Noticia general
Título: El crucial rol que juega el directorio en la gestión de la ciberseguridad en las empresas

Pág. : 12
Cm2: 930,8

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Es urgente que los directorios se aseguren de que sus organizaciones cuenten con políticas sólidas de seguridad digital, implementen controles internos adecuados y realicen evaluaciones periódicas de vulnerabilidades, dicen expertos. El llamado es a tomarse el tema "con la seriedad que merece".

SOFÍA MALUENDA

UN 55% NO TIENE O NO SABE SI CUENTA CON UN DIRECTOR CALIFICADO EN LA MATERIA:

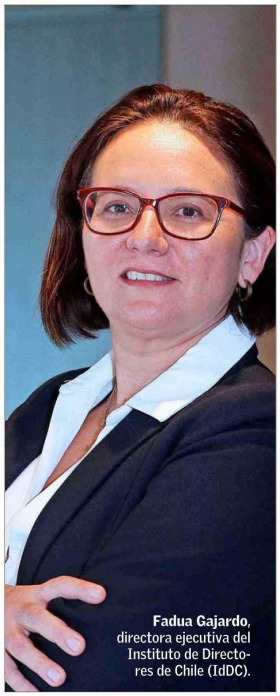
El crucial rol que juega el directorio en la gestión de la ciberseguridad en las empresas

El mundo se mueve aceleradamente y así también lo hace el cibercrimen, al que están expuestos tanto las personas como las empresas las 24 horas del día. Hace años, señala la directora de empresas Tina Rosenfeld, en los directorios empezaron a discutir sobre los riesgos que podrían afectar la seguridad física de las personas. "Hoy, ver que alguien se expone a situaciones riesgosas, que le podrían afectar su integridad física, es absolutamente inaceptable. Este cambio cultural se produjo en las organizaciones partiendo desde el directorio. Con el tema de ciberseguridad debería pasar lo mismo. Los directorios tienen que incluir con urgencia la revisión de los riesgos relacionados con los sistemas de información digital en su agenda anual. La ciberseguridad, al igual que la seguridad física, debería ser parte de la cultura de las compañías para asegurar la continuidad del negocio", asegura Rosenfeld.

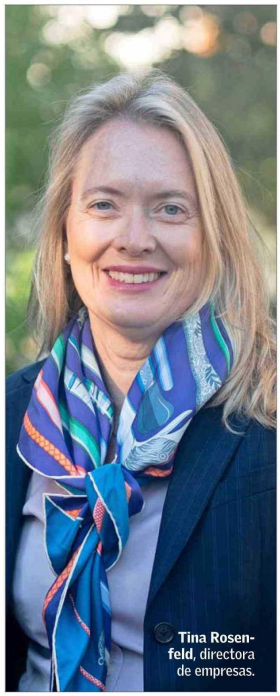
"La falta de conocimientos técnicos no exime a los directores de su responsabilidad. **Al contrario, deben buscar capacitación y asesoría especializada".**

FADUA GAJARDO
Directora ejecutiva del Instituto de Directores de Chile (IdDC).

"Es urgente que los directorios se aseguren de que sus organizaciones cuenten con políticas sólidas de ciberseguridad, implementen controles internos adecuados y realicen evaluaciones periódicas de vulnerabilidades. Asimismo, deben exigir reportes regulares sobre el estado de la ciberseguridad y los incidentes, incluso los menos críticos", sostiene Fadua Gajardo, directora ejecutiva del Instituto de Directores de Chile (IdDC). "Nuestro llamado es a tomarse este tema con la seriedad que merece. Las empresas y sus directorios deben tomar las precauciones necesarias frente a una amenaza cada vez más sofisticada. Como directores, nuestra responsabilidad es tener una visión integral de los desafíos empresariales, y la ciberseguridad es, sin duda, uno de los más urgentes", detalla.



Fadua Gajardo, directora ejecutiva del Instituto de Directores de Chile (IdDC).



Tina Rosenfeld, directora de empresas.

Ricardo Seguel, director del magíster en ciberseguridad de la UAI.

"Transformar la cultura organizacional a una organización cibersegura es un esfuerzo lento, complejo **y que tiene impacto positivo en el mediano y largo plazo".**

RICARDO SEGUEL
Director magíster ciberseguridad UAI.

RADIOGRAFÍA

Recientemente en el IdDC realizaron el estudio "Radiografía de la ciberseguridad de los directorios de Chile 2024", y si bien el panorama es mejor que en 2023, todavía quedan retos por resolver. "Uno de los resultados que más llama la atención es que a la espera de la entrada en vigor de la nueva Ley Marco de Ciberseguridad y la creación de la futura Agencia Nacional de Ciberseguridad (ANCI), aún son muchos los directorios en Chile que enfrentan retos en la gestión de los riesgos digitales. Si bien hay algunos avances, los directores, en su mayoría, desconocen el impacto que tendrá la regulación e incluso, no tienen claridad de las sanciones a las que se exponen las empresas", explica Gajardo sobre los resultados y detalla que esto se debe a que muchas veces los temas de seguridad digital no están abordados a nivel de directorios, sino en áreas o departamentos específicos. "Aquí hay un desafío de sensibilización y de involucrar estos temas en las agendas de los directorios para poder entender el impacto que va a tener esta aplicación en las compañías que nosotros representamos", asegura.

"Es vital que los directores nos capacitemos en forma constante para mantenernos actualizados".

TINA ROSENFELD
Directora de empresas.

En esa línea, otro reto es que los directorios cuenten con personas capacitadas en la materia. El estudio evidenció que un 45% de estos cuenta con al menos un integrante calificado en ciberseguridad, superando el 22% de la versión 2023. A pesar del avance, el 55% dijo que no tiene o no sabe si cuenta con un director calificado en la materia. "La falta de conocimientos técnicos no exime a los directores de su responsabilidad. Al contrario, deben buscar capacitación y asesoría especializada para tomar decisiones bien fundamentadas y resguardar la seguridad de la compañía", dice Gajardo. Por último, apenas un 19% de las empresas asigna un presupuesto "robusto" para ciberseguridad.

PRINCIPALES **RETOS**

Los desafíos a los que se enfrentan son múltiples. Ricardo Seguel, director del magíster en ciberseguridad de la Universidad Adolfo Ibáñez, señala que los principales son: "que los directores comprendan la prioridad estratégica de la ciberseguridad; que no es un gasto, sino que una inversión que va de la mano del apetito de riesgo que ellos definen anualmente, y que transformar la cultura organizacional a una organización cibersegura es un esfuerzo lento, complejo y que tiene impacto positivo en el mediano y largo plazo".

"El mayor desafío de los directorios es mapear bien los riesgos asociados al ciberespacio, sobre todo en un entorno cambiante, donde la innovación desafía constantemente, no solamente los procesos, sino también los sistemas y las personas", puntualiza Rosenfeld y agrega que la ciberseguridad tiene que estar presente en capacitaciones constantes para que todos, incluyendo los directores, entiendan la relevancia de un ambiente seguro. "Juegos de rol y simulaciones de ataques son una excelente herramienta para visibilizar las amenazas cibernéticas y poner a prueba los planes de continuidad de negocio", ejemplifica. "Es vital que los directores nos capacitemos en forma constante para mantenernos actualizados", agrega.

"No incluir la ciberseguridad en la estrategia del negocio es un riesgo muy grande para la sostenibilidad a largo plazo, ya que el aumento de los ciberataques y la dependencia digital exponen a las empresas a interrupciones operativas, pérdida de datos críticos y daño reputacional. Además, en un entorno regulatorio cada vez más estricto, las organizaciones que no implementen medidas adecuadas de seguridad pueden enfrentar sanciones y demandas legales que comprometen su viabilidad", asegura Gajardo. Menciona también cómo los directores de empresa deberán valorar incorporar perfiles con experiencia en la gestión de nuevas tecnologías de la información y con capacidad para elaborar las estrategias oportunas en términos de seguridad digital.

CINCO PREGUNTAS CLAVE QUE LOS DIRECTORES DEBEN REALIZARSE, SEGÚN EL IDDC:

1. ¿Es consciente el directorio de la variedad de riesgos a los que se enfrenta la compañía en materia de ciberseguridad y el potencial con el que cuenta para mejorar sus controles internos?; ¿cuentan los dispositivos y los sistemas usados por los directores, la dirección y el personal clave con el nivel de protección adecuado?
2. ¿Qué cambios se han implementado en el marco de control interno y procedimientos de supervisión de la ciberseguridad con motivo de la expansión del teletrabajo?, ¿la potencial mejora de la tecnología que protege los datos de la organización es debatida a nivel del directorio?
3. ¿Cuán preparada está la función interna de ciberseguridad de la organización?, ¿se necesitan más recursos, personal o mejora del *software*?
4. ¿Qué planes de contingencia están en marcha para responder ante una violación de la seguridad digital?, ¿cómo la dirección mantiene una respuesta eficaz a los incidentes y la recuperación de datos?
5. ¿Se están ejecutando protocolos de prevención y concienciación en la organización y cómo se manejan los riesgos de exposición de datos críticos en la relación con tanto *stakeholders* como proveedores?, ¿cómo son los pasos adicionales para lograr la protección colaborativa de la ciberseguridad?