GERENCIA
Tecnologías y estrategias para la transformación digital

Fecha: 31/10/2025 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $829.080 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $829.080 Difusión: 0
Vpe portada: $829.080 Ocupación: 100%



ESPECIAL

MES DE LA CIBERSEGURIDAD

## José Lagos, FEN Universidad de Chile

# "Invertir en ciberseguridad es invertir en estabilidad y reputación"

***La ciberseguridad dejó de ser un asunto exclusivamente técnico para transformarse en un factor de competitividad y confianza empresarial. En conversación con Revista Gerencia, José Lagos, director del Diplomado en Ciberseguridad de UEjecutivos de la Facultad de Economía y Negocios de la Universidad de Chile, analiza los desafíos que enfrentan las empresas chilenas ante el nuevo marco regulatorio, la brecha de talento y el impacto económico de los ciberataques.***

### ¿Cómo está afectando la ciberseguridad la competitividad y la productividad de las empresas?

Los incidentes de ciberseguridad y datos tienen efectos devastadores en las empresas, los que ya no se miden sólo por sus efectos técnicos, sino por su impacto económico, operacional, reputacional, cumplimiento y dependiendo del incidente, vidas humanas. Cada interrupción de sistemas, servicios o fuga de datos puede comprometer cadenas de suministro, elevar costos de seguros y erosionar gravemente la reputación de la empresa.

En este aspecto, la Ley 21.663 refuerza esa visión al exigir gobernanza técnica y coordinación público-privada. En consecuencia, la seguridad digital se convierte en motor de productividad, al proteger la disponibilidad de servicios, los activos intangibles y la estabilidad de las operaciones.

La triada de ciberseguridad, protección de datos e inteligencia artificial, debe mejorar la productividad y competitivas de las empresas en Chile. De lo contrario, nuestro crecimiento se verá afectado.

En el nuevo entorno regulatorio, invertir en ciberseguridad es invertir en estabilidad, reputación y acceso a mercados digitales más exigentes.

### ¿Se puede hablar hoy de una brecha de inversión en ciberseguridad entre grandes corporaciones y Pymes?

Es evidente la brecha existente de inversión entre las grandes empresas y las Pymes, la que puede variar desde un 20% del presupuesto, si comparamos la inversión en ciberseguridad con el presupuesto de tecnología, o menos del 1% en las Pymes.

Este desbalance o desequilibrio genera una concentración de vulnerabilidades en los eslabones más débiles de la cadena, especialmente en proveedores críticos. Aun cuando es importante considerar que la inversión óptima en ciberseguridad, no debe estar dada por el tamaño de la empresa, sino por su nivel de exposición al riesgo, y sobre todo del apetito al riesgo en ciberseguridad.

En la actualidad, las Pymes enfrentan tres desafíos: falta de capacidades internas, ausencia de economías de escala y desconocimiento regulatorio. Reducir la brecha digital exige democratizar el acceso a herramientas de protección y fomentar modelos de colaboración público-privada.

### Desde una mirada macroeconómica, ¿cómo impactan los ciberataques en la confianza digital y en el desarrollo del ecosistema empresarial?

Los ciberataques masivos tienen efectos macroeconómicos: reducen la confianza en los pagos digitales, frenan la adopción de soluciones GovTech, FinTech y e-Commerce, e impactan el crecimiento.

En términos de producto interno, incidentes críticos en sectores de energía, salud o banca podrían afectar entre 0,3 % y 0,6 % del PIB anual. Por último, el impacto del cibercrimen como un todo podría llegar al 2% del PIB.

La confianza digital es hoy un activo país. Fortalecerla implica alinear políticas públicas, gobernanza corporativa y educación tecnológica.

**Muchas empresas ven la ciberseguridad como un gasto y no como una inversión. ¿Cómo debería medirse su retorno o valor estratégico?**

El ROI de la ciberseguridad no se mide por ganancias directas, sino por riesgos evitados y valor estratégico. A modo de ejemplo, podríamos mencionar la reducción del tiempo de inactividad de un incidente (valor económico), o el cumplimiento de la Ley 21.663 (valor regulatorio) o la confianza de clientes y accionistas (valor reputacional). Medir la ciberseguridad como un seguro de continuidad operativa y resiliencia permite vincularla al control financiero y al rendimiento corporativo.

**¿Qué modelos o marcos de referencia recomienda para integrar la gestión del riesgo cibernético dentro del control financiero y operativo de una organización?**

En este sentido, es necesario implementar modelos de riesgos que permitan mantener un lenguaje financiero, y poder cuantificar la pérdida esperada que una empresa puede tener en caso de materialización de incidentes, por lo cual uno de los marcos más utilizados con una visión financiera. En este aspecto, es FAIR (Factor Analysis Information Risk). Para un aspecto operacional, la utilización de CIS18 e ISO 27.001, ISO 27.701, bajo la NIST CSF, podría ser una mezcla ideal. Las organizaciones maduras y líderes en este aspecto integran diversos framework bajo uno paragua, fácil de entender y comunicar al Directorio de las empresas.

**¿Qué papel están jugando la IA y la automatización en la detección y respuesta ante incidentes?**

La inteligencia artificial, específicamente modelos de IA generativa y sobre todo modelos de machine learning, ya están transformando la detección y respuesta a incidentes, lo que permite analizar grandes volúmenes de logs, identificando anomalías y ejecutando respuestas automatizadas.
Sin embargo, también introduce riesgos éticos y de dependencia algorítmica. La IA sin una cultura Digital madura no mejora la resiliencia, sólo automatiza errores.
La clave es avanzar hacia Modelos de Machine Learning explicables y auditados, integrados en equipos humanos capacitados y marcos regulatorios claros, en donde la clave deben ser los aspectos éticos y la participación humana en cada ciclo del modelo (Human in the Loop).

**¿Existen riesgos de dependencia tecnológica frente a soluciones de ciberseguridad internacionales? ¿Debería fomentarse el desarrollo local?**

Chile enfrenta el riesgo de dependencia tecnológica (vendor lock-in) respecto de proveedores internacionales, por lo cual es fundamental promover la interoperabilidad y desarrollo local. En este caso, las recomendaciones estratégicas se encaminan en requerir revisión local o código abierto en componentes críticos, fomentar la innovación público - privada y establecer incentivos a startups nacionales, que desarrollen soluciones de detección, respuesta o análisis forense.
La autonomía tecnológica es parte de la soberanía digital: Chile debe equilibrar cooperación global y desarrollo interno.

GERENCIA
Tecnologías y estrategias para la transformación digital

Fecha: 31/10/2025 Audiencia: 0 Sección: ACTUALIDAD
Vpe: $829.080 Tirada: 0 Frecuencia: MENSUAL
Vpe pág: $829.080 Difusión: 0
Vpe portada: $829.080 Ocupación: 100%



ESPECIAL

# MES DE LA CIBERSEGURIDAD

## ¿Hay una brecha de talento y capacidades en este campo?

El déficit de profesionales especializados supera los 15.000 puestos proyectados para 2025. La demanda se concentra en analistas SOC, auditores ISO 27001, ingenieros de respuesta a incidentes y CISOs certificados, por lo cual es necesario en diversos planos, tanto pregrado como postgrado, crear carreras que permitan satisfacer la demanda, lo cual no solo implica la creación de nuevas carreras, sino también Diplomas, Máster y Doctorados en Ciberseguridad. Pero antes, es necesario que los Máster estén acreditados y que más del 50% de los profesores tengan doctorados en temas a fines, con la finalidad de asegurar la calidad de la formación. Debemos ocuparnos fuertemente de la calidad de los programas actuales.

## ¿Qué efectos se puede esperar de la Ley Marco de Ciberseguridad?

En el corto plazo, la Ley 21.663 establecerá la infraestructura institucional, mejorará la higiene de ciberseguridad en muchas organizaciones, tanto de servicios esenciales y en especial de operadores vitales. Por otro lado, en el mediano plazo transformará la cultura empresarial hacia una gestión del riesgo cibernético integral y entenderá que la seguridad de la información, ciberseguridad y protección de datos personales y sensibles debe ser por diseño y defecto para operar en la economía digital.

## Haciendo una proyección a cinco años, ¿cómo ve el perfil de la empresa exitosa?

Las empresas chilenas más exitosas hacia 2030 compartirán cinco atributos clave:

**1.** Gobernanza digital: CISO con asiento en el directorio.

**2.** Integración del riesgo cibernético al ERM (financiero, operativo y reputacional).

**3.** Automatización responsable con IA explicable.

**4.** Cadena de valor segura con proveedores certificados.

***Medir la ciberseguridad como un seguro de continuidad operativa y resiliencia permite vincularla al control financiero y al rendimiento corporativo.***

**5.** Cultura organizacional comprometida con la seguridad y la continuidad. La resiliencia no será una ventaja competitiva, sino un requisito mínimo para operar en ecosistemas digitales globales. G