INSTITUTO DE DIRECTORES DE CHILE

Código de Buenas Prácticas en **Gobernanza Digital** para Chile

Con el apoyo de

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

Autores

Fadua Gajardo,
directora ejecutiva del Instituto de Directores de Chile
María Francisca Yáñez,
Directora de empresas
Gonzalo Medina,
Socio en Dal Pozzo Medina Abogados

Con el apoyo de Agencia Nacional de Ciberseguridad

Fecha de publicación Octubre 2025

Carta de presentación

Desde el Instituto de Directores de Chile, tenemos el agrado de presentar el **Código de Buenas Prácticas en Gobernanza Digital,** un documento elaborado para fortalecer el rol estratégico de los directorios frente a los desafíos y oportunidades que plantea la era digital. Este código ha sido especialmente adaptado al contexto chileno, considerando su realidad regulatoria, organizacional y cultural, con el propósito de orientar a los órganos de gobierno corporativo en la gestión responsable de los riesgos asociados a la ciberseguridad.

Vivimos en un escenario de transformación acelerada, impulsado por la adopción de tecnologías que redefinen la forma de operar, competir y tomar decisiones. Sin embargo, estas oportunidades traen consigo nuevos riesgos y responsabilidades. La ciberseguridad ya no puede abordarse solo como un asunto técnico; es un tema estratégico que exige liderazgo informado, pensamiento crítico y una cultura organizacional alineada con la protección de los activos digitales, la continuidad operativa y la confianza de los stakeholders.

Este código presenta acciones críticas y recomendaciones concretas para fortalecer la gobernanza cibernética desde el directorio, fomentando una visión preventiva y resiliente. Más que una guía técnica, este documento es un llamado a repensar los procesos de toma de decisiones y redefinir el rol del directorio frente a un cambio de paradigmas que demanda una gobernanza moderna, ética y visionaria.

Agradecemos especialmente el trabajo de **Gonzalo Medina** y **María Francisca Yáñez,** quienes participaron como coautores de este documento, aportando su experiencia, conocimiento y compromiso a lo largo de todo el proceso. Asimismo, expresamos nuestro sincero agradecimiento a la **Agencia Nacional de Ciberseguridad** por su respaldo y apoyo, contribuyendo de manera significativa a la calidad, pertinencia y orientación estratégica de este código.

Invitamos a los directores, ejecutivos y líderes del país a adoptar estas buenas prácticas como un paso decisivo hacia una gobernanza responsable que asegure la sostenibilidad a largo plazo de las compañías.

Fadua Gajardo
Directora Ejecutiva
Instituto de Directores de Chile

Carta Agencia Nacional de Ciberseguridad

La participación activa y el compromiso de los directores y directoras en materias de ciberseguridad es esencial para asegurar la resiliencia y la responsabilidad de las instituciones en un entorno cada vez más digitalizado. A medida que los procesos operativos, administrativos y estratégicos dependen totalmente de tecnologías interconectadas, los riesgos asociados a incidentes de ciberseguridad crecen en complejidad, impacto y costos.

El rol del directorio resulta determinante para orientar políticas y estrategias, asignar los recursos adecuados y asegurar que las decisiones estratégicas consideren la protección tanto de los activos tecnológicos como de los datos de clientes y trabajadores. Cuando la alta dirección de una organización asume un compromiso explícito con la ciberseguridad, se establece un marco claro de prioridades y se refuerza la importancia de gestionar los riesgos digitales al mismo nivel que otros riesgos críticos de la organización.

Un directorio informado y dotado de las herramientas necesarias puede anticipar amenazas, comprender mejor la naturaleza de los incidentes y promover una cultura organizacional que incorpore la seguridad digital en todos los niveles. Este enfoque no solo impulsa la adopción de medidas básicas que toda persona dentro de la institución debe cumplir, sino que también facilita la implementación de prácticas avanzadas destinadas a proteger procesos altamente sensibles.

Desde la Agencia Nacional de Ciberseguridad compartimos la necesidad de tomar decisiones con la mayor información disponible y por ellos hemos lanzado las 9 medidas básicas de ciberseguridad que cualquier organización no importando su tamaño debiera implementar para mejorar su seguridad digital, que está disponible en el sitio web https://anci.gob.cl/9basicos

Los *9 básicos de la ciberseguridad* complementan perfectamente el código de buenas prácticas del IDC, porque ambos instrumentos facilitan la comprensión de los riesgos emergentes, ofrecen criterios de gobernanza y ayudan a estandarizar buenas prácticas, permitiendo que cada institución avance de manera ordenada y alineada con estándares reconocidos.

Daniel Álvarez Valenzuela
Director Nacional
Agencia Nacional de Ciberseguridad

Introducción

Código de Buenas Prácticas en Gobernanza Digital ha sido diseñado para apoyar a los directorios y sus miembros en la adecuada gobernanza de los riesgos de ciberseguridad. Este documento presenta las acciones críticas que deben implementar los directorios, adaptado para su aplicabilidad en el contexto chileno.

A. Gestión de riesgos

A.1	Obtener garantías de que los procesos tecnológicos críticos han sido identificados y priorizados.
A.2	Velar por que la organización identifique tanto riesgos de daño cibernético a la propia organización, como potenciales afectaciones de terceros.
A.3	Acordar la propiedad ejecutiva de los riesgos cibernéticos y asegurar su integración en la gestión de riesgos empresariales.
A.4	Definir y comunicar el apetito de riesgo cibernético, asegurando la existencia de un plan de acción correspondiente.
A.5	Asegurar que los riesgos del ecosistema de proveedores y socios comerciales sean evaluados proporcionalmente.
A.6	Realizar evaluaciones periódicas de riesgos que consideren los cambios regulatorios y tecnológicos.

B. Estrategia

B.1	Asegurar que exista una estrategia de ciberseguridad alineada con la estrategia organizacional.
B.2	Verificar que dicha estrategia cumple con regulaciones vigentes y se adapta al contexto cambiante.
B.3	Asegurar la asignación efectiva de recursos para cubrir los riesgos cibernéticos identificados.
B.4	Velar por la evaluación respectoa la correcta ejecucion de la estrategia se y genere los resultados esperados.

C. Personas

C.1	Promover una cultura organizacional de ciberseguridad basada en comportamientos positivos y responsabilidad.
C.2	Validar que existan políticas claras que respalden dicha cultura.
C.3	Realizar capacitación para mejorar la alfabetización cibernética de los directores.
C.4	Asegurar la existencia de programas de formación y concienciación efectivos y medibles.

D. Planificación, respuesta y recuperación ante incidentes

D.1	Verificar que exista un plan de respuesta y recuperación ante incidentes cibernéticos.
D.2	Asegurar ejercicios anuales del plan que incluyan actores internos y externos relevantes.
D.3	En caso de incidente, asumir obligaciones regulatorias y apoyar decisiones clave.
D.4	Garantizar procesos de revisión post-incidente que alimenten mejoras continuas.

E. Supervisión y aseguramiento

E.1	Establecer una estructura de gobernanza cibernética clara y con roles definidos.
E.2	Exigir reportes periódicos y métricas alineadas con la estrategia cibernética.
E.3	Fomentar el diálogo entre directores y ejecutivos clave como el CISO.
E.4	Integrar la ciberseguridad en auditorías y mecanismos de aseguramiento existentes.
E.5	Validar que los ejecutivos estén al tanto de regulaciones y mejores prácticas.

F. Ciberhigiene: Directores como protagonistas

Los miembros del directorio no solo supervisan la ciberseguridad: también son un objetivo privilegiado de los atacantes. En la era digital, la identidad es la nueva frontera de seguridad. Adoptar medidas básicas de higiene digital puede reducir más del 90% del riesgo, de acuerdo con estudios de organismos internacionales y la industria.

Recomendaciones esenciales

- Usar un gestor de contraseñas para proteger credenciales y evitar contraseñas repetidas o débiles.
- Activar Doble Factor de Autenticación (MFA) en todos los accesos sensibles.
- Contar con una plataforma segura para la gestión y comunicación de materias sensibles del directorio (nunca correo personal ni WhatsApp).

Nota: Estas recomendaciones tecnológicas se basan en las mejores prácticas vigentes, pero **deben revisarse y actualizarse periódicamente**, ya que la tecnología, las amenazas y las soluciones evolucionan con rapidez.