



CIBERSEGURIDAD:

MÁS COBERTURA EFECTIVA PARA UNA PROTECCIÓN INTEGRAL

Con la nueva ley de protección de datos se pasa de un modelo principalmente declarativo a uno basado en responsabilidad activa y trazabilidad. En paralelo, la tecnología sigue avanzando en la aplicación de nuevas herramientas que resguarden de mejor manera los contenidos y traspaso de información de carácter informático.

En un mundo cada vez más globalizado y en el que la tecnología juega cada vez un papel más preponderante, la protección de datos en *data centers*, transacciones de cualquier tipo y traspaso de información resulta fundamental. En especial si se considera que al día son millones los intercambios informáticos que se realizan con estas características y que los hackers también han desarrollado nuevas técnicas para apoderarse de datos e información de los usuarios.

Al respecto se refiere Marco Antonio Perelli, profesor asociado en Duoc UC sede Plaza Norte y experto en todo lo que diga relación con ciberseguridad y redes. Además es especialista en gobernanza, ciberseguridad, gestión del cambio organizacional y cumplimiento regulatorio, asesorando a empresas en la implementación de sistemas de seguridad y protección de datos alineados a estándares y normativa vigente.

—¿Cuáles son los alcances de la nueva ley de protección de datos y qué cambia en relación a la anterior?

“La Ley 21.719 moderniza completamente el sistema chileno de protección de datos personales. A diferencia de la antigua Ley 19.628, establece principios más claros, mayores obligaciones para las organizaciones, un régimen sancionatorio más robusto y crea la Agencia de Protección de Datos Personales como autoridad especializada. El cambio central es que ya no basta con declarar buenas prácticas, las organizaciones

deben implementar medidas concretas de gestión, seguridad y gobernanza interna que permitan demostrar cumplimiento. Se pasa de un modelo principalmente declarativo a uno basado en responsabilidad activa y trazabilidad”.

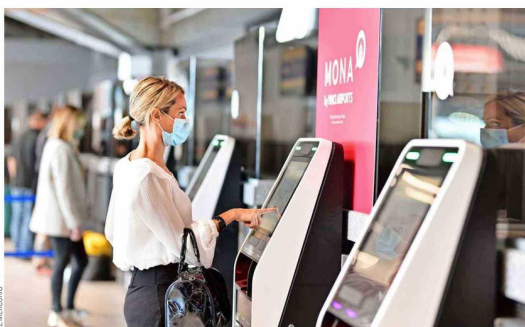
—¿Cómo se define el concepto de DPO y cuál es su aplicación práctica?

“El Delegado de Protección de Datos (DPO) es la figura encargada de supervisar el cumplimiento de la normativa dentro de la organización. Su función es asesorar en materia de protección de datos, promover políticas internas, apoyar la gestión de riesgos y actuar como referente interno en estas materias. En la práctica, el DPO estructura el sistema de cumplimiento: impulsa registros, procedimientos, capacitación y coordinación entre áreas técnicas, legales y operativas. No es un rol simbólico, sino una función estratégica orientada a integrar la protección de datos en la gestión organizacional”.

MÁS RIESGOS Y MÁS SOLUCIONES

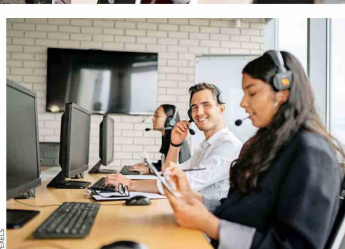
—¿Qué sectores son más críticos en cuanto a la necesidad de protección de datos y por qué?

“Los sectores que manejan grandes volúmenes de datos o información sensible, como salud, banca, telecomunicaciones, educación, comercio electrónico y sector público. El riesgo no depende solo de la cantidad de datos, sino del impacto que puede generar su uso indebido, fraude,



Marco Antonio Perelli, profesor asociado en Duoc UC sede Plaza Norte.

suplantación de identidad, extorsión o afectación de derechos. También son relevantes los entornos con múltiples proveedores, donde el tratamiento de datos se



extiende a lo largo de una cadena de actores, aumentando la superficie de riesgo”.

—¿Cuáles son las últimas tecnologías en materia biométrica y ciberseguridad?

“En biometría destacan tecnologías de detección de vida (*liveness*), que permiten evitar suplantaciones mediante fotos o *deepfakes*, y la biometría conductual, que analiza patrones de uso para reforzar la autenticación. Por su parte en

ciberseguridad, se consolida el enfoque Zero Trust, la autenticación sin contraseña mediante *passkeys* y la segmentación de redes. También avanzan las herramientas de prevención de fuga de datos y cifrado avanzado.

La tendencia apunta a integrar identidad, monitoreo continuo y control de accesos para proteger la información de manera integral”.

—¿Cómo se incorpora la IA en la demanda de protección de datos?

“La inteligencia artificial incrementa la demanda de protección de datos porque permite recolectar, analizar e inferir información a gran escala, muchas veces generando perfiles y decisiones automatizadas que pueden impactar derechos de las personas. En Chile, además, se observa un uso creciente y masivo de herramientas de IA por parte de profesionales y organizaciones, quienes con frecuencia cargan información en estas plataformas sin evaluar adecuadamente si contienen datos personales o información sensible. Esto puede generar transferencias no controladas y riesgos legales relevantes.

Dado todo lo anterior, la protección de datos debe incorporarse desde el diseño de sistemas y procesos, mediante evaluación de riesgos, minimización de datos y control estricto de accesos. El desafío es equilibrar innovación tecnológica con responsabilidad y resguardo efectivo de derechos”.