

RIC 14 y edificios inteligentes

La eficiencia energética ya no se juega solo en el tablero eléctrico



Por Alejandro Palma, Of Counsel de Magliona Abogados, experto en energías.

La entrada en vigencia del RIC 14 no solo eleva las exigencias de eficiencia energética en edificios, sino que también instala nuevos desafíos en materia de datos, accesos y ciberseguridad. En un entorno cada vez más automatizado, la operación eficiente de una edificación depende tanto de sus sistemas eléctricos como de la solidez con que se gobierna su infraestructura digital.

debe incorporar gobernanza de datos y ciberseguridad como parte del diseño.

RIC 14: eficiencia con una nueva capa de información

RIC 14 apunta precisamente en esa dirección, aunque muchas veces se lo lea solo desde la lógica del cumplimiento eléctrico. La norma exige medición separada de consumos relevantes en edificios nuevos, registros periódicos, conservación de información por un tiempo mínimo y entrega de documentación operativa al propietario o administrador. Incluso considera elementos especialmente sensibles desde una perspectiva digital, como los diagramas del sistema monitoreado o controlado, los manuales de usuario y mantenimiento, las llaves de acceso a tableros y las credenciales de ingreso a software. Es decir, la eficiencia energética regulada ya viene acompañada de una capa de administración de información y accesos.

Ese punto es clave. Cuando un edificio comienza a operar sobre la base de monitoreo continuo, no solo administra energía: también procesa información sobre uso de espacios, horarios, hábitos de ocupación, eventos de acceso, funcionamiento de equipos, mantenciones y trazabilidad operativa. A veces esos

datos parecerán meramente técnicos. Pero cuando pueden vincularse con personas identificadas o identificables, con credenciales, con patrones de presencia o incluso con sistemas biométricos o de geolocalización integrados, entramos en un terreno regulatorio distinto. Allí ya no basta con que la solución funcione bien; debe, además, tratar los datos de forma lícita, con finalidad determinada, medidas de seguridad adecuadas y criterios claros de conservación y transparencia. Chile, además, está entrando en una etapa regulatoria más exigente. La Ley N° 21.719, publicada en 2024 y con entrada en vigencia prevista para diciembre de 2026, elevó de manera sustantiva el estándar de protección de datos personales. Introduce principios como licitud, finalidad, responsabilidad, seguridad y transparencia, y presta especial atención a categorías sensibles como datos de salud, biométricos, geolocalización y datos de niños, niñas y adolescentes. Para los edificios inteligentes, esto tiene consecuencias prácticas inmediatas: obliga a preguntarse qué datos se recogen realmente, para qué, por cuánto tiempo, con qué base de licitud, quién accede a ellos y bajo qué contratos o instrucciones operan los proveedores tecnológicos.

(Continúa en página 22)

(Viene de página 20)

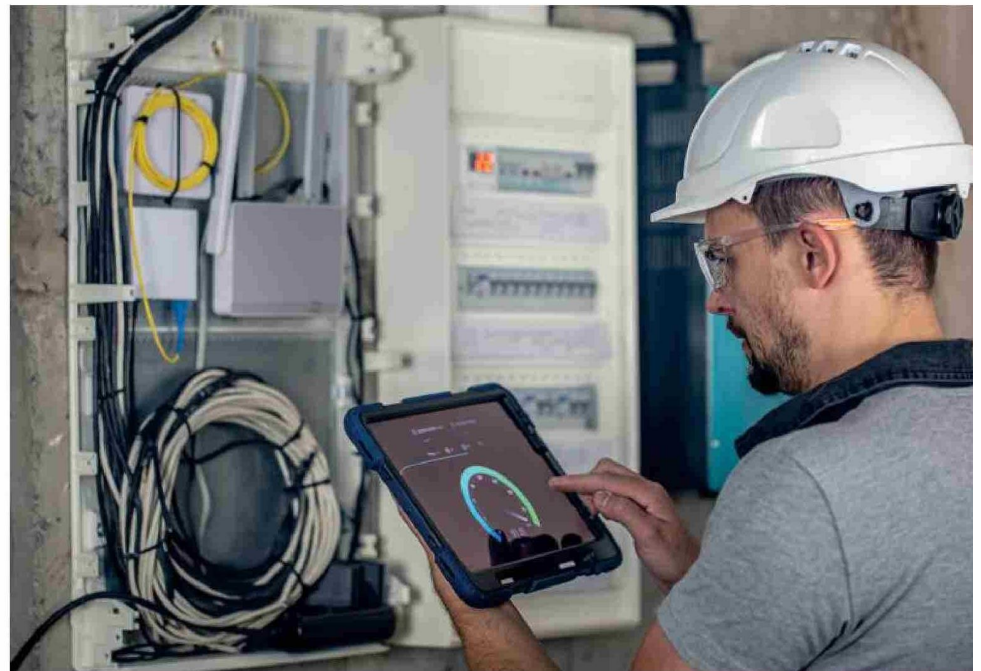
La ciberseguridad ya no puede entrar al final del proyecto

La segunda dimensión es la ciberseguridad. En demasiados proyectos todavía se entiende como una capa posterior, casi decorativa, que se agrega al final de la implementación. Ese enfoque es riesgoso. En un edificio inteligente, un incidente no solo compromete confidencialidad; también puede afectar integridad y disponibilidad. Si se altera un sistema de monitoreo, si se degradan las credenciales de administración, si se interrumpe la comunicación entre subsistemas o si un tercero mantiene accesos remotos mal gobernados, el impacto no será únicamente informático: puede traducirse en sobreconsumo, fallas operacionales, interrupciones de servicio, exposición de ocupantes o decisiones erradas de mantenimiento.

La Ley Marco de Ciberseguridad, N° 21.663, refuerza esa lectura. Su lógica no se limita a reaccionar ante ataques: exige medidas permanentes para prevenir, reportar y resolver incidentes, y contempla deberes reforzados para operadores de importancia vital, incluyendo gestión continua, continuidad operacional y reducción del impacto de incidentes. Aunque no todo edificio quedará comprendido en esas categorías, la señal regulatoria es inequívoca: la seguridad digital de los sistemas que soportan servicios esenciales o procesos críticos ya no puede tratarse como un problema exclusivamente técnico. Es una exigencia de gestión, continuidad y responsabilidad.

Gobernar la infraestructura digital para sostener la eficiencia

Por eso, el desafío para inmobiliarias, operadores, facility managers, integradores, comunidades, industrias y grandes usuarios no es solo “cumplir RIC 14”, sino gobernar la infraestructura digital que ese cumplimiento ayuda a desplegar. Eso exige, al menos, cinco decisiones tempranas: inventariar activos y flujos de datos; definir propietarios internos de la información y de los accesos; seg-



En edificios inteligentes, eficiencia, datos y ciberseguridad dejaron de ser conversaciones separadas.

mentar redes y administrar privilegios de terceros; establecer contratos y anexos con obligaciones de seguridad, soporte, actualización y respuesta a incidentes; y diseñar políticas de conservación, anonimización o eliminación cuando los datos ya no sean necesarios. Sin esa base, la automatización promete eficiencia, pero también multiplica opacidad y riesgo.

En este punto, la experiencia comparada ya es clara: los proyectos más sólidos no son los que acumulan más hardware, sino los que integran arquitectura, operación, legalidad y seguridad desde el inicio. La interoperabilidad sin gobierno produce dependencia. La automatización sin trazabilidad produce vulnerabilidad. Y la analítica sin reglas de acceso, finalidad y retención produce un pasivo regulatorio que tarde o temprano emerge, ya sea por fiscalización, conflicto contractual, incidente de seguridad o cuestionamiento reputacional.

El edificio verdaderamente inteligente no es el que enciende o apaga sistemas

de manera automática. Es el que puede demostrar que usa la tecnología para consumir mejor, operar mejor y proteger mejor. En la nueva etapa de eficiencia energética, el indicador ya no será solo cuánta energía se ahorra, sino también cuán robusta es la gobernanza que sostiene ese ahorro. RIC 14 puede ser leído, entonces, no solo como una exigencia técnica, sino como una señal de madurez: en edificios inteligentes, eficiencia, datos y ciberseguridad dejaron de ser conversaciones separadas. ■

