LITORALPRESS

Fecha: 21-05-2026
Medio: El Heraldo
Supl. : El Heraldo
Tipo: Noticia general
Título: **Teletrabajo sin resguardos**

Pág. : 2
Cm2: 459,6

Tiraje: 3.000
Lectoría: 6.000
Favorabilidad: No Definida

Teletrabajo sin resguardos

Durante la pandemia, el teletrabajo dejó de ser una modalidad excepcional para transformarse, de un día para otro, en la regla. Aunque el escenario sanitario ya quedó atrás, el trabajo remoto o híbrido sigue siendo una realidad instalada, tanto en Chile como en el mundo. Sin embargo, la discusión pública se ha concentrado más en la productividad o en la conciliación laboral, dejando en segundo plano una dimensión crítica: la ciberseguridad.

Trabajar desde una oficina institucional no es lo mismo que hacerlo desde el comedor de la casa. En las organizaciones, los funcionarios operan sobre redes corporativas protegidas, con firewalls, monitoreo permanente, segmentación de accesos y políticas de seguridad claramente definidas. En contraste, el teletrabajo suele apoyarse en redes domésticas, muchas veces mal configuradas, compartidas con otros dispositivos y usuarios, y sin estándares mínimos de protección. Esa brecha no es solo técnica: es un riesgo real.

En Chile, el teletrabajo tuvo su punto más alto en 2020, cuando alcanzó cerca del 20% de las personas ocupadas. Sin embargo, esa cifra cayó de forma sostenida tras la pandemia. Según datos de la Subsecretaría del Trabajo y el Observatorio del Contexto Económico de la Universidad Diego Portales, en 2023 solo un 4% de los trabajadores mantenía una modalidad plenamente remota, equivalente a unas 278 mil personas. Aun así, el trabajo híbrido permanece como una fórmula habitual en sectores administrativos, académicos y de servicios.

La conclusión es clara: aunque Chile presenta una adopción acotada, el teletrabajo sigue siendo estructural y no una anomalía pasajera.

El gran riesgo es asumir que trabajar desde casa es simplemente "llevarse el computador". En realidad, se rompe el perímetro de seguridad tradicional. En el hogar, los dispositivos institucionales suelen conectarse a redes Wi-Fi con contraseñas débiles, routers sin actualizar, ausencia de cifrado adecuado o incluso redes compartidas con televisores inteligentes, cámaras IP y teléfonos móviles.

Este escenario amplía exponencialmente la superficie de ataque. No es casual que el 69% de las organizaciones latinoamericanas haya reportado al menos un incidente de seguridad en el último año, siendo el phishing, el robo de credenciales y el malware las principales amenazas. El trabajo remoto, sin políticas claras y controles técnicos adecuados, actúa como un acelerador del riesgo.

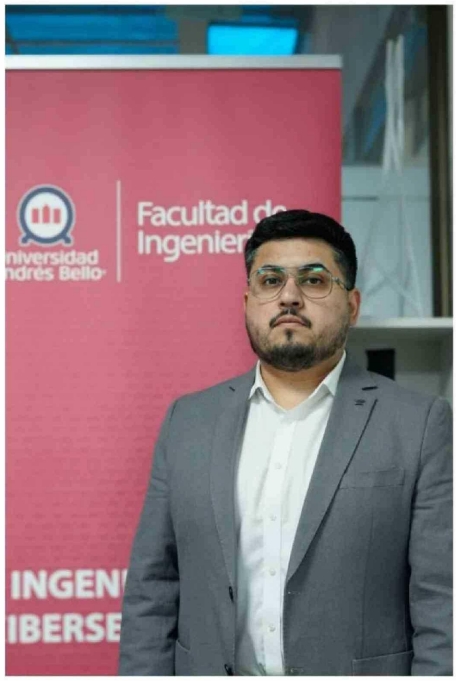
Además, informes recientes advierten que en América Latina los ciberataques han aumentado de forma sostenida, con más de 291 víctimas de ransomware en 2024, un 15% más que el año anterior, y con un volumen masivo de credenciales filtradas en la región. Cada trabajador remoto mal protegido es, potencialmente, un punto de ingreso para este tipo de ataques.

A la debilidad técnica se suma un factor humano. En la oficina, existen controles visibles, accesos segmentados, autenticación multifactor, soporte técnico inmediato. En casa, en cambio, es común compartir equipos, reutilizar contraseñas o conectarse a redes abiertas "por comodidad". No es mala fe; es falta de conciencia digital.

Los estudios regionales coinciden en que muchas organizaciones han avanzado en normativas de teletrabajo, pero no al mismo ritmo en capacitación en ciberseguridad, evaluación de riesgos ni provisión de herramientas seguras como VPN corporativas o autenticación multifactor obligatoria.

Cuestionar los riesgos del teletrabajo no significa abogar por su eliminación. Significa, más bien, asumir que la casa no es una extensión natural de la red institucional. Si el trabajo remoto llegó para quedarse, también deben quedarse los resguardos: políticas claras, inversión en infraestructura segura y formación continua de los trabajadores.

La pregunta, entonces, no es si el teletrabajo es bueno o malo, sino si estamos dispuestos a tomarnos en serio su dimensión digital. Porque cuando la ciberseguridad se descuida, el costo no lo paga el router doméstico: lo paga la institución, la confianza pública y, muchas veces, la información de todos.



Edgardo Fuentes Cáceres - Director Ingeniería en Ciberseguridad, UNAB