LITORALPRESS

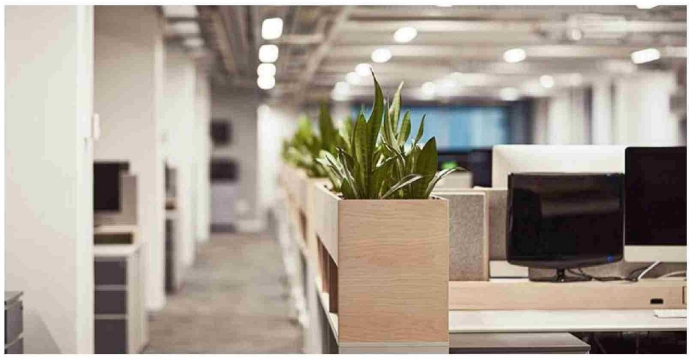
Fecha: 09-01-2026
Medio: El Heraldo
Supl. : El Heraldo
Tipo: Noticia general
Título: Riesgo digital en verano: ¿ por qué las empresas quedan más expuestas a ciberataques en vacaciones?

Pág. : 9
Cm2: 483,8

Tiraje: 3.000
Lectoría: 6.000
Favorabilidad: No Definida

Riesgo digital en verano: ¿por qué las empresas quedan más expuestas a ciberataques en vacaciones?

Con equipos reducidos y menor monitoreo, los entornos digitales críticos de las empresas, como sitios web, aplicaciones y bases de datos, quedan más expuestos durante el período estival. Expertos advierten que un incidente puede escalar en horas, afectar gravemente la confianza de los usuarios y generar consecuencias legales.



El verano es sinónimo de descanso, equipos reducidos y turnos más cortos. Sin embargo, mientras muchas empresas "desconectan", los riesgos digitales no se toman vacaciones. Durante este período, la disminución de personal y la menor supervisión operativa incrementan las brechas de seguridad, dejando a sitios web, aplicaciones móviles y bases de datos corporativas con menor monitoreo y convirtiéndolos en un blanco atractivo para ciberataques, filtraciones de datos o usos indebidos de información sensible.

Los especialistas advierten que este escenario es cada vez más frecuente y que un incidente de ciberseguridad puede impactar de forma directa la continuidad del negocio, además de dañar la reputación corporativa, la confianza de los usuarios y exponer a las organizaciones a sanciones regulatorias y legales.

Uno de los riesgos menos visibles, pero igual de relevantes, es el uso indebido de plataformas digitales corporativas para fines distintos a los autorizados. Esto puede incluir desde accesos no controlados hasta la utilización de canales oficiales para difundir información sensible o no autorizada, un escenario especialmente crítico cuando no existen mecanismos de detección temprana, y que se vuelve aún más delicado en contextos como procesos electorales o campañas públicas.

"Hoy la pregunta no es si una empresa será atacada, sino cuándo y qué tan preparada estará para responder", explica Herwin Cajamarca, gerente de ingeniería de negocios de IFX Chile, empresa especializada en soluciones IT para compañías en América Latina.

Apps, sitios web y datos: los puntos más vulnerables

Las aplicaciones móviles, los sitios web y las bases de datos concentran gran parte de la información crítica de las empresas y de sus clientes. Sin un monitoreo continuo y especializado, estos canales pueden transformarse rápidamente en la puerta de entrada para ataques o filtraciones que escalan en pocas horas y derivan en una crisis pública.

En este contexto, soluciones como SOCaaS (Security Operations Center como Servicio) permiten a las empresas contar con monitoreo permanente y en tiempo real de servidores, aplicaciones y dispositivos críticos, detectando comportamientos anómalos antes de que el incidente se haga visible o tenga impacto en los usuarios finales. Este servicio es gestionado de forma continua por equipos especializados de IFX, las 24 horas del día, los 7 días de la semana, lo que permite actuar de manera temprana, coordinar la respuesta con la organización afectada y contener el incidente de forma oportuna.

"No se trata solo de prevenir ataques, sino de asegurar la continuidad operacional y proteger la confianza de los clientes", señala Cajamarca.