LITORALPRESS

Fecha: 21-04-2026
Medio: Contraplano Reñaca-Concón-Quintero-Puchuncavi-Zapa
Supl. : Contraplano Reñaca-Concón-Quintero-Puchuncavi-Zapa
Tipo: Noticia general
Título: Ciberseguridad en crisis: grave vulnerabilidad en cuentas digitales del Presidente Kast expone fallas en el uso de credenciales

Pág. : 101
Cm2: 734,4

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

Ciberseguridad en crisis: grave vulnerabilidad en cuentas digitales del Presidente Kast expone fallas en el uso de credenciales

Ciberseguridad vuelve a instalarse en el centro del debate público tras el acceso indebido a cuentas digitales asociadas al Presidente José Antonio Kast, un episodio que reabre la discusión sobre las debilidades en la administración de perfiles institucionales y el uso responsable de credenciales dentro del aparato estatal.

La ciberseguridad en cuentas institucionales volvió al centro del debate tras un incidente que afectó perfiles oficiales vinculados al Mandatario, evidenciando vulnerabilidades que van más allá de un posible ataque sofisticado. Para el ingeniero informático y especialista Patricio Campos, el problema principal no radica únicamente en la acción de terceros, sino en una gestión deficiente de accesos digitales, especialmente cuando múltiples personas administran una misma cuenta.

El experto explicó que, en estos escenarios, el riesgo aumenta considerablemente debido a la falta de control sobre quién conoce las credenciales, cómo se almacenan

LITORALPRESS

Fecha: 21-04-2026
Medio: Contraplano Reñaca-Concón-Quintero-Puchuncavi-Zapa
Supl. : Contraplano Reñaca-Concón-Quintero-Puchuncavi-Zapa
Tipo: Noticia general
Título: Ciberseguridad en crisis: grave vulnerabilidad en cuentas digitales del Presidente Kast expone fallas en el uso de credenciales

Pág. : 102
Cm2: 737,6

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

y con qué frecuencia se actualizan. La ciberseguridad deja así de ser un asunto técnico aislado para transformarse en una responsabilidad estructural que involucra prácticas organizacionales y protocolos claros de administración.

Uno de los puntos más críticos es el hábito de compartir contraseñas entre integrantes de un equipo, una práctica común en entornos operativos pero que constituye una de las mayores vulnerabilidades en sistemas digitales. Cuando varias personas utilizan las mismas credenciales, se pierde trazabilidad y se debilita el control interno, dificultando la identificación de responsabilidades ante una eventual filtración o acceso indebido.

En este contexto, el especialista comparó esta práctica con entregar la llave de una bóveda a múltiples personas, aumentando inevitablemente el riesgo de pérdida, copia o exposición. Por ello, insistió en la necesidad de implementar protocolos estrictos, segmentación de permisos y monitoreo constante en la gestión de cuentas institucionales, especialmente en organismos públicos.

Otro aspecto clave es la ausencia o insuficiencia de autenticación multifactor, una herramienta considerada hoy esencial en cualquier sistema de protección digital. Campos recalcó que una contraseña por sí sola ya no es suficiente, y que la incorporación de una segunda capa de verificación puede marcar la diferencia entre un intento fallido y una vulneración efectiva con consecuencias institucionales.

Asimismo, advirtió sobre la reutilización de contraseñas en distintas plataformas, una práctica que amplifica los riesgos, ya que una filtración en un servicio menor puede abrir acceso a cuentas más sensibles. En el ámbito gubernamental, esta debilidad adquiere mayor gravedad al comprometer no solo información, sino también la confianza pública en la seguridad de los sistemas del Estado.

El análisis también abordó la posibilidad de hacktivismo o participación de actores externos con motivaciones políticas, aunque el especialista fue enfático en señalar que muchos incidentes tienen un origen más simple: errores humanos, falta de protocolos y malas prácticas acumuladas en el tiempo. Este diagnóstico pone el foco en la necesidad de fortalecer la cultura digital dentro de las instituciones.

En materia de investigación, Campos explicó que existen herramientas de análisis forense digital para rastrear responsabilidades, pero también múltiples obstáculos, como el uso de redes privadas virtuales o sistemas de ocultamiento que dificultan la trazabilidad. Esto refuerza la idea de que la prevención es más efectiva que la reacción, ya que una vez ocurrido el incidente, el impacto reputacional y político ya está en curso.

El caso deja en evidencia que el Estado chileno enfrenta desafíos complejos en materia de ciberseguridad, debido a la diversidad de organismos, niveles de acceso y sistemas existentes. La implementación de estándares homogéneos requiere coordinación, inversión y disciplina, elementos clave para fortalecer la protección de las plataformas institucionales.

En definitiva, la ciberseguridad se posiciona como un desafío urgente que trasciende lo técnico, demandando formación continua, normas claras y una gestión rigurosa de accesos. Más que una amenaza externa, muchas vulnerabilidades se originan en prácticas internas, recordando que en el entorno digital, una pequeña falla puede escalar rápidamente hasta convertirse en una crisis de gran magnitud.