CPLT refuerza ciberseguridad de Portal de Transparencia del Estado usado por más de mil cien instituciones públicas

El Consejo para la Transparencia está impulsando acciones de refuerzo de seguridad digital en el Portal de Transparencia del Estado que utilizan más de mil cien organismos públicos del país. Lo anterior, con el objetivo de proteger los accesos, ordenar el uso de claves y prevenir problemas que puedan afectar la atención de solicitudes de información pública que dirigen las personas a dichos organismos o bien la publicación de información exigida por la Ley de Transparencia.

La medida apunta a acciones concretas, tales como que las instituciones revisen quiénes de sus funcionarios tienen acceso al portal, eliminen usuarios que ya no correspondan, actualicen permisos, eviten compartir claves y reporten rápidamente cualquier situación sospechosa.

Actualmente, el Portal de Transparencia del Estado reúne a 1.102 organismos públicos, entre ellos servicios de la Administración Central del Estado, gobiernos regionales, municipalidades, corporaciones y asociaciones municipales, y otras instituciones obligadas por la Ley de Transparencia. A modo de ejemplo, y para comprender la magnitud del tráfico digital que se desarrolla a través de este sitio, solo en abril de 2026 registró más de 821 mil visitas y 32.528 solicitudes de acceso a información pública fueron dirigidas por su intermedio.

Desde el CPLT explicaron que el objetivo es simple: reforzar la ciberseguridad de una de las principales puertas digitales que tiene la ciudadanía para pedir información al Estado y revisar antecedentes que deben estar disponibles permanentemente.

La presidenta del Consejo para la Transparencia, Natalia González, señaló que “cuando hablamos de transparencia, también hablamos de confianza. Si miles de personas usan este portal para revisar o solicitar información pública, es fundamental que los organismos mantengan sus accesos ordenados, sus claves protegidas y sus usuarios actualizados. Son medidas simples, pero muy importantes para cuidar el funcionamiento del sistema y el adecuado resguardo de información institucional”.

El trabajo impulsado por el Consejo considera recomendaciones prácticas para los equipos encargados de transparencia, entre ellas: usar contraseñas robustas y únicas, no compartir credenciales, revisar periódicamente los usuarios activos, asignar permisos solo a quienes realmente los necesitan y eliminar accesos de personas que dejaron de cumplir funciones vinculadas al portal.

También se pidió a los organismos públicos reforzar el cuidado frente a correos sospechosos, no abrir enlaces desconocidos, usar equipos y redes de wifi institucionales y reportar de inmediato cualquier actividad extraña como accesos no autorizados o *malware, phishing o smishing*.

Desde el Consejo señalaron que esta iniciativa forma parte de una línea de trabajo orientada a mejorar los estándares de seguridad, disponibilidad y confianza de los canales digitales de transparencia. Para ello, el organismo continuará incluyendo estas temáticas en sus capacitaciones habituales, a fin de orientar y compartir buenas prácticas con las instituciones públicas que utilizan esta plataforma.