Sala Constitucional

Resolución Nº 32917 - 2025

Fecha de la Resolución: 10 de Octubre del 2025 a las 09:20
Expediente: 25-024824-0007-CO
Redactado por: Jorge Araya Garcia
Clase de asunto: Recurso de amparo
Analizado por: SALA CONSTITUCIONAL

Indicadores de Relevancia
Sentencia relevante

Sentencia con datos protegidos, de conformidad con la normativa vigente

---

Contenido de Interés:
Tipo de contenido: Voto de mayoría
Rama del Derecho: 4. ASUNTOS DE GARANTÍA
Tema: TRABAJO
Subtemas:

- TELETRABAJO.

032917-25. SE CUESTIONA LA OBLIGACIÓN DE SUTEL A SUS FUNCIONARIOS, DE INSTALAR EN SUS DISPOSITIVOS MÓVILES PERSONALES, UNA APLICACIÓN DE DOBLE FACTOR DE AUTENTICACIÓN, PARA PODER REALIZAR TELETRABAJO (WATHGUARD AUTHPOINT). SE DECLARA SIN LUGAR, AL ESTAR FRENTE A UNA DECISIÓN INSTITUCIONAL SUSTENTADA EN CRITERIOS TÉCNICOS. RGS10/2025
Se declara sin lugar el recurso.-
"(…) este Tribunal Constitucional no considera que exista mérito para acoger este proceso de amparo. Lo anterior, por lo motivos que se explicarán a continuación.

A. En cuanto a la decisión de utilizar sistema de doble factor de autenticación mediante el uso de una aplicación instalada en los teléfonos móviles personales de los funcionarios de la SUTEL que desean realizar teletrabajo (y no mediante el uso de tokens físicos). Tema de mera legalidad. Según se logra desprender con meridiana claridad del estudio del informe rendido por la parte recurrida y del elenco de hechos probados, el Consejo de la SUTEL acordó en julio de este año 2025 que aquellos funcionarios que deseen acogerse al teletrabajo debían instalar en sus teléfonos móviles personales una aplicación de doble factor de verificación como mecanismo de seguridad. También se demostró que, aun cuando se podría utilizar tokens físicos para tales efectos, la autoridad recurrida se decantó finalmente por la instalación de la referida aplicación en los teléfonos celulares de los funcionarios. Según se consignó, la Unidad de Tecnología de Información de la SUTEL determinó, con base en criterios técnicos y de costo-beneficio, que el método de autenticación multifactor se implementaría mediante una aplicación móvil. En consuno con lo anterior, el Presidente del Consejo y representante judicial y extrajudicial de la Superintendencia de Telecomunicaciones sostuvo en el informe rendido que *"(…) la decisión de no considerar tokens físicos responde a un análisis técnico y de adopción previa, Asimismo, se consideró que el uso de esa herramienta en los dispositivos móviles es la mejor opción por temas de eficiencia, costo y versatilidad para todas las partes (…)".*
Analizado lo anterior, esta Sala Constitucional considera que no le corresponde –por tratarse de un tema de pura y mera legalidad–, realizar un análisis por el fondo, concretamente, respecto a los criterios técnicos que respaldan el uso de mecanismos de autenticación multifactor mediante la instalación propiamente de una aplicación electrónica o bien, mediante el uso de token físico y determinar finalmente cuál de estos es el más apropiado o adecuado a efecto de lograr los fines señalados por la SUTEL. Tampoco, le corresponde a esta jurisdicción cuestionar el criterio de oportunidad y conveniencia de la administración recurrida para utilizar el factor de doble autenticación mediante la instalación de una aplicación en los celulares y no permitir el uso de tokens físicos. Mucho menos, desde esa perspectiva, podría este Tribunal finalmente acoger la pretensión del recurrente y ordenarle a la SUTEL dejar sin efecto la disposición en cuestión y permitirle, en su caso y excepcionalmente, hacer uso del token físico.
Claramente estamos frente a una decisión institucional sustentada en múltiples criterios e informes técnicos (tal y como se comprobó en el apartado de hechos probados de esta sentencia), respecto a la cual el tutelado se encuentra disconforme y respecto a la cual, si a bien lo tiene, puede plantear los alegatos que estime pertinentes ante las vías ordinarias de legalidad administrativas y jurisdiccionales creadas especialmente al efecto.

B. Fundamentación de la decisión reclamada. Cabe destacar que la decisión de la SUTEL respecto a la cual se encuentra disconforme el recurrente (obligación de instalar en su celular personal una aplicación de doble factor de autenticación llamada AuthPoint de WatchGuard), no se encuentra carente de sustento ni se podría tildar *prima facie* de arbitraria. Por el

contrario, se ha demostrado que dicha medida se ha gestionado e implementado por motivos de seguridad y en aras de prevenir ataques cibernéticos y garantizar el resguardo, protección e integridad de los datos y equipos propiedad de la institución. En cuanto a este aspecto, en el oficio No. 01480-SUTEL-UJ-2025 de 20 febrero de 2025 suscrito por parte de la Unidad Jurídica de la SUTEL se consignó lo siguiente

*"(…) **el objetivo es fortalecer la seguridad de la información y proteger los datos sensibles y equipos de la SUTEL**. Asimismo, el fin de la herramienta de seguridad indicada, se deriva de las diversas directrices emitidas por el MICITT y el criterio técnico de la Unidad de Tecnologías de Información de la SUTEL (…)*

el uso de la doble autenticación a través de dispositivos móviles se presenta como una solución adecuada para mitigar el riesgo en la vulneración de equipos, sistemas y dato de la entidad (…)

Las herramientas solicitadas son instrumentos básicos para la protección de la información institucional y el resguardo de la operación técnica de la SUTEL (…)

***La herramienta de autenticación multifactor (MFA) es fundamental para reforzar la seguridad en el acceso a sistemas y datos sensibles.** Al requerir múltiples formas de verificación más allá de las contraseñas, como códigos temporales o notificaciones push, el MFA **reduce el riesgo de violaciones de seguridad, protege la información confidencial y cumple con regulaciones del Código Nacional de Tecnologías Digitales Capítulo 2 Identificación y Autenticación Ciudadana. Además, en un entorno laboral remoto, garantiza un acceso seguro desde ubicaciones externas**. Esta capa adicional de seguridad no solo fortalece la protección de datos, sino que también mejora la experiencia del usuario al proporcionar un acceso seguro sin comprometer la usabilidad una vez que se integra adecuadamente (…)"* (El destacado no forma parte del original).

Por su parte, el Presidente del Consejo y representante de la Superintendencia de Telecomunicaciones aseveró en su informe lo siguiente:

*"(…) Cabe recalcar que el **no implementar el método de doble factor de autenticación (2FA) representa un riesgo crítico para la seguridad de la información en cualquier organización**. Confiar únicamente en contraseñas expone a los sistemas institucionales a ataques comunes como el phishing, el robo de credenciales, o el uso de contraseñas reutilizadas, facilitando accesos no autorizados a información sensible, servicios críticos o recursos internos. Este tipo de brechas puede derivar en pérdida de información confidencial, continuidad operativa, daño reputacional e incluso sanciones regulatorias, especialmente en el sector de gobierno como lo es SUTEL. **La implementación de 2FA mitiga significativamente estos riesgos al requerir una segunda forma de verificación mediante una aplicación autenticadora**. Esto bloquea vectores de ataque como el robo de contraseñas, los intentos de fuerza bruta, y los accesos indebidos incluso si las credenciales han sido comprometidas. **Adoptar 2FA es una de las medidas más efectivas y de bajo costo para fortalecer la postura de ciberseguridad y proteger tanto a los usuarios como a la organización** (…)*

*la Unidad de Tecnologías de Información (…) emitió el criterio técnico que justifica la implementación de la herramienta denominada WatchGuard Authpoint en los dispositivos móviles personales de los funcionarios, como requisito para realizar el doble factor de autenticación y permitir a los funcionarios laborar en la modalidad de teletrabajo. **De dicho criterio técnico, se extrae que el requerimiento en análisis tiene como objetivo principal velar por el interés público, al fortalecer la seguridad de la información y proteger los datos sensibles y equipos de la Sutel ante las continuas violaciones y hackeos de información que se han dado a nivel nacional**. Asimismo, la implementación de la herramienta de seguridad indicada **se deriva de las diversas directrices y lineamientos emitidos por el MICITT y el MIDEPLAN, que, provienen de marcos regulatorios que rigen a todas las instituciones públicas** (…)"* El destacado no forma parte del original).

Aunado a ello, no puede perderse de vista que la obligación impuesta a los funcionarios recurridos tiene sustento, a su vez, en la normativa que regula el teletrabajo. En ese particular, en el citado oficio No. 01480-SUTEL-UJ-2025 de 20 febrero de 2025, la Unidad Jurídica de la SUTEL explicó lo siguiente:

"(…) La Ley para regular el teletrabajo, Ley N° 9738, aplica para la Sutel, según lo que establece el artículo 2. Por lo tanto, es aplicable lo dispuesto en el artículo 9 inciso a) que establece lo siguiente: "Artículo 9- Obligaciones de las personas teletrabajadoras. Sin perjuicio de las demás obligaciones que acuerden las partes en el contrato o adenda de teletrabajo, serán obligaciones para las personas teletrabajadoras las siguientes: a) Cumplir con los criterios de medición, evaluación y control determinados en el contrato o adenda, así como sujetarse a las políticas y los códigos de la empresa, respecto a temas de relaciones laborales, comportamiento, confidencialidad, manejo de la información y demás disposiciones aplicables."

El Reglamento para regular el teletrabajo, decreto Nº 42083-MP-MTSS-MIDEPLAN-MICITT, en el artículo 6 establece los deberes de las personas teletrabajadoras y indica que las personas teletrabajadoras deben cumplir lo siguiente: b) Las demás obligaciones contenidas en el contrato o adenda de teletrabajo y la legislación costarricense.

De acuerdo con esa ley y reglamento, es una obligación de las personas que teletrabajan cumplir con las políticas que emita la institución, por lo que, esas normas se deben complementar con las regulaciones emitidas por la Sutel El Reglamento de Teletrabajo en la Autoridad Reguladora de los Servicios Públicos y su órgano desconcentrado (en adelante Reglamento de Teletrabajo), el cual resulta aplicable a SUTEL, dispone en lo relevante lo siguiente: "Artículo 5.- Dependencias de apoyo de la CIT y sus funciones. Son dependencias de apoyo las que a continuación se indican y tendrán las funciones siguientes: (…) b) Tecnologías de Información, se encargará de: (…) 4) Definir, actualizar y comunicar oportunamente las condiciones mínimas de tecnologías de información y comunicación con las que debe contar la persona teletrabajadora en el centro o lugar de teletrabajo, incluidas las medidas de seguridad informática".

De conformidad con el reglamento antes citado, el establecimiento de condiciones mínimas en tecnologías de información que la Unidad de Tecnología de Información (en adelante UTI) defina mediante criterio técnico para personas que, voluntariamente, desean acceder a la modalidad de teletrabajo, se encuentra contemplado en la normativa específica que aplica a la SUTEL, por lo que resulta posible. Además, se destaca que el Reglamento de Teletrabajo contempla las obligaciones del funcionario en teletrabajo y, en lo que interesa dispone lo siguiente: "Artículo 2. Alcance. El presente reglamento es de acatamiento obligatorio

para todas las personas funcionarias de la Autoridad Reguladora de los Servicios Públicos y su órgano desconcentrado que voluntariamente soliciten la aprobación del teletrabajo como una modalidad de trabajo a distancia mediante el uso de medios y tecnología de la información y comunicación (…) Artículo 6. - Condiciones generales del teletrabajo. Las condiciones generales del teletrabajo son las siguientes: (…) e) Requiere el uso y cumplimiento de las condiciones mínimas vigentes establecidas por tecnologías de información y salud ocupacional en el lugar o centro de teletrabajo para acceder a la modalidad de teletrabajo. (…) ***Artículo 10.- Requisitos de la persona teletrabajadora. La persona funcionaria que solicite el teletrabajo deberá cumplir con cada uno de los requisitos siguientes: (…) d) Cumplir con los lineamientos específicos emitidos por la CIT y las dependencias de apoyo en materia de tecnologías de la información y comunicación y de salud ocupacional. (…)***
Artículo 12.- Obligaciones de la persona teletrabajadora (…) b) Tramitar una adenda al contrato de teletrabajo en caso de que varíe alguna de las condiciones que justificaron su ingreso a la modalidad de teletrabajo (lugar o centro de teletrabajo estipulado, cambio de puesto, actividades o condiciones mínimas de tecnologías de información y salud ocupacional requeridas, así como el cambio permanente en los días de teletrabajo estipulados). El teletrabajo se continuará realizando hasta que se apruebe la adenda al contrato (…)".
Lo anterior implica que, una vez que se defina algún requerimiento mínimo en tecnologías de información como requisito para acceder a la modalidad de teletrabajo de parte de UTI, los colaboradores que deseen estar en dicha modalidad deben cumplir con ese requisito *(…)"* (El destacado no forma parte del original).

C. Sobre la presunta violación a lo dispuesto en el ordinal 24 constitucional. Como punto medular de este amparo, el recurrente manifiesta que la instalación de la aplicación en cuestión en su teléfono celular (aplicación AuthPoint de WatchGuard como mecanismo de doble factor de autenticación), violenta sus derechos a la intimidad y a la autodeterminación informativa. Particularmente, sostiene que desconoce el alcance de sus funciones y la interacción que podría tener con otras aplicaciones y datos personales del funcionario que se encuentran en su móvil. Alega que se podría permitir el acceso a datos e información vinculada a los celulares, tales como geolocalización, desplazamientos e, incluso, en algunos casos, datos relacionados con la salud y la condición física del titular del aparato.
No obstante, esta Sala no estima de recibido este agravio. Primero, por cuanto el tutelado no hizo referencia a un hecho en concreto (con sustento probatorio), sino a un hecho futuro e incierto, sea, sobre la eventual posibilidad de que, al instalársele la aplicación bajo estudio, se acceda a su información personal contenida en el celular. Como bien lo informó la parte recurrida, se trata de meras suposiciones o conjeturas que no fueron respaldadas, además, con ningún fundamento o sustento técnico y probatorio. Segundo, dado que, contrario a lo que sostiene el recurrente, el Presidente del Consejo de la Superintendencia de Telecomunicaciones informó bajo juramento (con sustento en varios oficios y pruebas adjuntas), que, a través de dicha aplicación, no se acceden a los datos que reclama el tutelado.
En ese particular, es importante señalar que en el oficio No. 09751-SUTEL-DGO-2024 de fecha 4 de noviembre de 2024 suscrito por la Jefatura de la Unidad Jurídica y la Jefatura de la Unidad de Tecnologías de Información de SUTEL, se consignó, al respecto, lo siguiente:
"(…) 4. DE LA HERRAMIENTA CONTRATADA MEDIANTE EL PROCEDIMIENTO DE CONTRATACIÓN NO. 2023LE-000002-00149000 B. DE LAS CARACTERÍSTICAS DE LA HERRAMIENTA Es importante recalcar que, la herramienta utiliza como método de autenticación, el dispositivo móvil, celular o smartphone, mediante la aplicación Authpoint y que, se utiliza, exclusivamente, para que el usuario valide su identidad al acceder a los sistemas. Mediante una sola aplicación, se puede validar el acceso a la computadora, a las herramientas colaborativas de Microsoft, como Teams y Outlook y, por último, la VPN.
Adicionalmente, se debe aclarar que ***la herramienta no tiene las siguientes funcionalidades: determinar la ubicación del dispositivo, realizar una intrusión en el sistema operativo del dispositivo móvil donde se instala u obtener información privada del funcionario, es únicamente, un método para verificar la identidad del funcionario*** *(…)"* (El destacado no forma parte del original).

Por su parte, en el oficio No. 01480-SUTEL-UJ-2025 de 20 febrero de 2025, la Unidad Jurídica de la SUTEL consignó:
"(…) se debe aclarar que la ***medida de seguridad de doble factor de autenticación no es un gestor de información personal ni tiene como uso técnico el análisis de información contenida en los dispositivos que lo instalen****, por lo que resulte importante citar la siguiente opinión remitida la UTI: "Las herramientas de autenticación de doble factor (2FA) son esenciales para fortalecer la seguridad de los sistemas y proteger a la institución contra accesos no autorizados. A diferencia de las contraseñas tradicionales, que pueden ser robadas o descifradas, el 2FA añade una capa adicional de seguridad, exigiendo un segundo factor de verificación, como un código de una aplicación o un mensaje push, antes de conceder acceso. Los ciberdelincuentes emplean diversas técnicas para robar credenciales, entre ellas: Ataques de fuerza bruta: Intentos automatizados para descifrar contraseñas mediante combinaciones masivas. Phishing: Engaños a los usuarios para que revelen credenciales a través de correos electrónicos, mensajes o sitios web falsos. Keylogging: Malware que registra las pulsaciones del teclado para capturar contraseñas y otros datos sensibles. Ataques de intermediario (Man-in-the-Middle): Interceptación del tráfico entre el usuario y el servidor para robar credenciales. Credential stuffing: Uso de combinaciones de usuario y contraseña filtradas en otras plataformas para intentar acceder a nuevos servicios. Para mitigar estos riesgos, se ha implementado la aplicación WatchGuard, que establece las siguientes condiciones en dispositivos móviles: (…) Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico El contenido generado por IA puede ser incorrecto. Permiso para envió de notificaciones push para conexiones con computadoras, VPN u Office 365. Acceso a la cámara solo para la activación, mediante lectura del código QR. (No pide grabación y/o fotografías del rostro del funcionario) Este permiso lo requieren la mayoría de las aplicaciones en el mercado, solo para citar las más relevantes a nivel institucional: Microsoft Authenticator y a nivel personal, Google Authenticator, Whatsapp y redes sociales en general requieren este tipo de permisos. Además este permiso se puede quitar luego de la instalación de la herramienta si así lo desea el usuario, debido a que es requerido únicamente para la lectura del código QR que asocia la cuenta al dispositivo.* ***La aplicación no contempla permisos de acceso a archivos, fotos, ni otros datos personales disponibles, en los dispositivos en los cuales se va a instalar.***

Además el funcionamiento descrito en la ficha técnica de la solución adquirida no incluye el acceso a datos personales, sensibles para su funcionamiento. *(…) A pesar de estas medidas, la ciberseguridad es un campo dinámico en constante evolución. Si bien ninguna solución garantiza protección absoluta, la implementación de herramientas como el doble o múltiple factor de autenticación reduce significativamente los riesgos y fortalece la seguridad de la información institucional (…)". (Correo electrónico del 20 de febrero del año en curso). De conformidad con lo antes expuesto, es procedente indicar que* ***el doble factor de autenticación no tiene como fin: gestionar, regular o utilizar información sensible de quienes lo instalen, por lo que carece de relación con aquellas garantías previstas en el artículo 24 de la C.P****. Además, se destaca que la instalación de la herramienta establece las condiciones de uso, mediante las cuales los eventuales usuarios se ven debidamente informados de los accesos de la aplicación (…)"* (El destacado no forma parte del original).

Igualmente, la autoridad recurrida aportó a este proceso un oficio de fecha 11 de agosto de 2025 suscrito por el proveedor Tecnova Soluciones S.A. en el cual, sobre el tema bajo estudio, se indicó lo siguiente:
"(…) En respuesta la consulta sobre la Privacidad del Usuario mencionada en el Anexo 1 del documento RECURSO DE RECONSIDERACIÓN AL ACUERDO N°005-042-2025 DEL 31 DE JULIO DEL 2025, detallamos los siguientes puntos: 1. La Política de Privacidad de Datos de la Aplicación WatchGuard Authpoint se encuentra publicada en el siguiente sitio oficial de WatchGuard Technologies: hLps://www.watchguard.com/es/wgrd-trust-center/privacy-guide/authpoint La consulta de la Política de Privacidad siempre es un recurso obligatorio a la hora de presentar cualquier recurso que tenga que ver con el manejo de datos privados del usuario. 2. Watchguard Technologies cumple la política GDPR de la Unión Europea para todos sus productos, puede encontrar el enunciado en el siguiente sitio web: hLps://www.watchguard.com/es/wgrd-trust-center/gdpr-statement A su vez también publica un Addendum sobre el Procesamiento de Datos de Clientes: hLps://www.watchguard.com/es/wgrd-trust-center/watchguard-technologies-inccustomer-data-processing-addendum 3. La imagen 3 del Anexo muestra un método equivocado para obtener los permisos de acceso de la aplicación WatchGuard Authpoint o cualquier otra aplicación: (…) La forma correcta es acceder a esa misma pantalla y seleccionar los tres puntos ubicados en la esquina superior derecha y seleccionar "Todos los permisos". Esa opción muestra la lista completa de permisos a las que tienen acceso las aplicaciones: (…) Por ejemplo, esta es la lista de permisos totales de la aplicación MicrosoZ Excel en el mismo smarphone, donde se evidencia el acceso a recursos como "have full network access" sin que esto signifique un riesgo de seguridad para el usuario: (…) 4. En cuanto al análisis del APK de Watchguard Authpoint, se parte de una premisa incorrecta: que la simple presencia de términos técnicos en el código de una aplicación equivale a una acción maliciosa. Este enfoque carece de rigor técnico y conduce a conclusiones erróneas y alarmistas que no se corresponden con la realidad operativa de la aplicación.
Muy específicamente detallamos los siguientes puntos remitiendo directamente a la Guía de Privacidad oficial de WatchGuard:
a. Sobre la Geolocalización y el supuesto "rastreo": *i. El análisis sugiere que la aplicación funciona como un "rastreador". Esto es categóricamente falso. La propia política de WatchGuard es explícita: la recopilación de geolocalización precisa (GPS) es opcional y requiere el consentimiento explícito del usuario. Si como usuario no se autoriza este permiso, la función simplemente no se activa. Su único fin, en caso de que una empresa decida usarla, es añadir capas de seguridad adicionales, como permitir autenticaciones solo desde una ubicación específica (por ejemplo permitir las autenticaciones solo desde Costa Rica).*
b. Sobre la supuesta Captura de Datos Biométricos (Huella/Rostro): *i. Según lo explica la guía de privacidad lo explica sin ninguna ambigüedad en la sección "Acceso a identificación biométrica": "No obtenemos acceso a los datos biométricos en sí ni los procesamos." ii. La aplicación utiliza la interfaz segura del sistema operativo del smartphone (Android o iOS). Cuando un usuario pone su huella, el sistema operativo es el que la verifica y únicamente le envía a la app una respuesta de "sí" o "no". La huella dactilar del usuario o sus datos faciales nunca salen de su dispositivo ni son visibles para WatchGuard o para el administrador de la aplicación WatchGuard Authpoint.*
c. Sobre los Permisos de Cámara y Red*: como indica la documentación, los permisos tienen fines justificados y limitados: i. Cámara: Se usa únicamente para que el usuario escanee el código QR al momento de registrar su dispositivo. No hay otra funcionalidad asociada. ii. Red/IP: Es indispensable. La aplicación necesita conectarse a internet para validar en tiempo real que eres tú quien intenta acceder a un servicio protegido. La IP se utiliza, como se ve en la tabla de "Fines del procesamiento", para mejorar la seguridad y detectar intentos de acceso no autorizados. iii. Términos como ip, address, Location o HLpURLConnection son extremadamente comunes en cualquier aplicación que se conecte a internet o utilice servicios de Google. Están presentes en librerías estándar de Android y Google Play Services. Encontrar 84,656 coincidencias de "Red/IP" no significa que la aplicación tenga 84,656 funciones para espiar la IP; significa que el código utiliza librerías de red estándar.*
Reiteramos que WatchGuard AuthPoint es una herramienta segura, confiable y transparente, diseñada exclusivamente para proteger los accesos corporativos, no para invadir la privacidad de los usuarios, y está certificada como tal *(…)"* (El destacado no forma parte del original).

En la resolución No. RCS-188-2025 de 21 de agosto de 2025 (emitida con motivo de una impugnación formulada por el recurrente y otros funcionarios de la SUTEL), el Consejo de la SUTE señaló también lo siguiente en cuanto al alegato relacionado con la presunta violación a la privacidad y a la protección de datos personales:
"(…) ***Considerando lo antes dispuesto, se debe aclarar que la medida de seguridad de doble fator de autenticación no es un gestor de información personal ni tiene como uso técnico el análisis de información contenida en los dispositivos que lo instalen****, por lo que resulte importante citar la siguiente opinión remitida la UTI: ---------- "Las herramientas de autenticación de doble factor (2FA) son esenciales para fortalecer la seguridad de los sistemas y proteger a la institución contra accesos no autorizados. A diferencia de las contraseñas tradicionales, que pueden ser robadas o descifradas, el 2FA añade una capa adicional de seguridad, exigiendo un segundo factor de verificación, como un código de una aplicación o un mensaje push, antes de conceder acceso. ---------- Los ciberdelincuentes emplean diversas técnicas para robar credenciales, entre ellas: ---------- Ataques de fuerza bruta: Intentos automatizados para descifrar contraseñas mediante combinaciones masivas.---------- Phishing: Engaños a los*

*usuarios para que revelen credenciales a través de correos electrónicos, mensajes o sitios web falsos. ---------- Keylogging: Malware que registra las pulsaciones del teclado para capturar contraseñas y otros datos sensibles. ---------- ---------- Ataques de intermediario (Man-in-the-Middle): Interceptación del tráfico entre el usuario y el servidor para robar credenciales. ---------- Credential stuffing: Uso de combinaciones de usuario y contraseña filtradas en otras plataformas para intentar acceder a nuevos servicios. ---------- Para mitigar estos riesgos, se ha implementado la aplicación WatchGuard, que establece las siguientes condiciones en dispositivos móviles: ---------- (…) Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico ---------- El contenido generado por IA puede ser incorrecto. ---------- ---------- Permiso para envió de notificaciones push para conexiones con computadoras, VPN u Office 365. ---------- ---------- **Acceso a la cámara solo para la activación, mediante lectura del código QR. (No pide grabación y/o fotografías del rostro del funcionario)** Este permiso lo requieren la mayoría de las aplicaciones en el mercado, solo para citar las más relevantes a nivel institucional: Microsoft Authenticator y a nivel personal, Google Authenticator, Whatsapp y redes sociales en general requieren este tipo de permisos. **Además este permiso se puede quitar luego de la instalación de la herramienta si así lo desea el usuario, debido a que es requerido únicamente para la lectura del código QR que asocia la cuenta al dispositivo. - La aplicación no contempla permisos de acceso a archivos, fotos, ni otros datos personales disponibles, en los dispositivos en los cuales se va a instalar**. Además el funcionamiento descrito en la ficha técnica de la solución adquirida no incluye el acceso a datos personales, sensibles para su funcionamiento. --- Lo anterior extraído de la página web: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/authpoint/mobile-app_see-device-info.html A pesar de estas medidas, la ciberseguridad es un campo dinámico en constante evolución. Si bien ninguna solución garantiza protección absoluta, la implementación de herramientas como el doble o múltiple factor de autenticación reduce significativamente los riesgos y fortalece la seguridad de la información institucional (…)". (Correo electrónico del 20 de febrero del año en curso). ---------- ---------- **De conformidad con lo antes expuesto, es procedente indicar que el doble factor de autenticación no tiene como fin: gestionar, regular o utilizar información sensible de quienes lo instalen, por lo que carece de relación con aquellas garantías previstas en el artículo 24 de la C.P**., sin embargo, se destaca que la instalación de la herramienta establece las condiciones de uso, mediante las cuales los eventuales usuarios se ven debidamente informados de los accesos de la aplicación (…)"* (El destacado no forma parte del original).

De esta manera, se demuestra también que al recurrente ya le han explicado que la aplicación no accede o manipula información personal y sensible del usuario.
En ese mismo orden de consideraciones, cabe destacar que, de forma contundente, el Presidente del Consejo y representante judicial y extrajudicial de la Superintendencia de Telecomunicaciones, informó bajo la solemnidad de juramento a esta Sala, lo siguiente:
*"(…) dicha aplicación puede ver la siguiente información del dispositivo móvil: datos técnicos del dispositivo móvil; permiso para envío de notificaciones push para conexiones con computadoras, VPN u Office 365 y; acceso a la cámara solo para la activación, mediante lectura del código QR (cabe recalcar que no pide grabación y/o fotografías del rostro del funcionario). Este permiso lo requieren la mayoría de las aplicaciones en el mercado, solo para citar las más relevantes a nivel institucional: Microsoft Authenticator y a nivel personal, Google Authenticator, Whatsapp y redes sociales en general requieren este tipo de permisos. **Además, este permiso se puede quitar luego de la instalación de la herramienta si así lo desea el usuario, debido a que es requerido únicamente para la lectura del código QR que asocia la cuenta al dispositivo. Cabe agregar que la aplicación no contempla permisos de acceso a archivos, fotos, ni otros datos personales disponibles, en los dispositivos en los cuales se va a instalar. Aunado a esto, el funcionamiento descrito en la ficha técnica de la solución adquirida no incluye el acceso a datos personales, sensibles para su funcionamiento**. Lo anterior, la UTI lo extrajo de la página web: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/authpoint/mobile-app_see-device-info.html y además, este criterio técnico se hizo constar en el oficio emitido por la jefatura de la Unidad de Tecnologías de Información y de la Unidad Jurídica de la Sutel, número 09751-SUTEL-DGO-2024 del 4 de noviembre de 2024 y en el oficio 01480-SUTEL-UJ-2025, emitido el 20 de febrero del 2025 por la Unidad Jurídica (…)*
*De conformidad con lo antes expuesto, **es posible concluir con meridiana claridad que el doble factor de autenticación no gestiona, regula o utiliza información sensible de quienes lo instalen, por lo que no trasgrede las garantías reguladas en el artículo 24 de la Constitución Política**. Además, dicha aplicación establece las condiciones de uso, mediante las cuales los eventuales usuarios se ven debidamente informados de los accesos de la aplicación (…)"* (El destacado no forma parte del original).

Finalmente, es importante apuntar que, en este caso, resulta aplicable lo dispuesto por este Tribunal, por ejemplo, en el Voto No. 2023-29772 de las 09:30 hrs. de 17 de noviembre de 2023; ocasión en la cual se señaló lo siguiente:
*"(…) **III.- Sobre el caso concreto.** En el sub examine, el recurrente asevera que el 9 de junio de 2023 fue publicado el cartel de licitación mayor nro. 2023LY-000025-0001000001: ADQUISICIÓN DE TAGS RFID, EQUIPOS Y SERVICIOS PARA MARCHAMO DIGITAL en el Sistema Integrado de Compras Públicas. Afirma que el objeto de la licitación es la contratación para la compra de "stickers" que contienen un chip de radiofrecuencia RFID; este sería utilizado a partir de 2024 por todos los vehículos en lugar de la actual calcomanía de marchamo. Reclama que tal dispositivo permitirá el rastreo y monitoreo de las personas e incidirá en la protección de datos. Acusa que no existe ley previa que autorice tal proceder, lo que es necesario cuando se trata del derecho a la intimidad (artículo 24 constitucional).*
*Ahora bien, la Sala considera que los reclamos planteados no pueden prosperar por varios motivos. **La Sala destaca que el accionante plantea una situación hipotética, que dista de ser una amenaza cierta, actual e inminente contra derechos fundamentales** (véase, verbigracia, la resolución nro. 2018-017621 de las 10:10 horas del 23 de octubre de 2018). **Si se obviara este obstáculo procesal, el recurso tampoco encontraría acogida en la Sala, toda vez que los informes rendidos desvirtúan los planteamientos del accionante**. Así, en lo que respecta al rastreo y monitoreo de las personas, se tuvo por probado que la contratación versa sobre etiquetas RFID pasivas, que no permiten trazar la trayectoria de un vehículo ni establecer la posición de*

un vehículo en un conjunto de lecturas sucesivas. No cuentan con un sistema de referencia de posición global. En cuanto a la información que incluiría la etiqueta RFID, se indicó que sería la misma que contiene el actualmente el marchamo físico (información que está disponible para cualquier persona que lea la calcamonía que se pega en el parabrisas del vehículo). Además, el acceso a la información de la etiqueta RFID requeriría un dispositivo especial, homologado por la SUTEL, por lo que se resguardaría del uso no autorizado (…)" (El destacado no forma parte del original).

D. Inexistencia de gestiones sin atender. En el escrito de interposición de este amparo, el tutelado señala que desconoce varios aspectos relacionados con la instalación y uso de la aplicación de doble factor de autenticación en cuestión y reclama que SUTEL ha omitido pronunciarse al respecto. Asimismo, señala que el Consejo de SUTEL no ha emitido un pronunciamiento expreso sobre los motivos por los cuales no se considera su propuesta (en cuanto a utilizar otro mecanismo de autenticación). No obstante, estos argumentos no son de recibo, en el tanto el recurrente no señaló o alegó que un determinado día haya presentado alguna gestión ante la recurrida relacionada con tales temas. Tampoco, aportó prueba alguna sobre el particular. Cabe agregar que la única gestión planteada (recurso de reconsideración y solicitud de medica cautelar), fue resuelta incluso antes de notificado este amparo a la parte recurrida.

E. Sobre la presunta sanción impuesta. En cuanto a este agravio, conviene señalarle al tutelado que, a la luz de las argumentaciones *supra* señaladas y explicadas en este considerando, no observa la Sala que el hecho de haberse señalado su nombre como parte de las personas que se opusieron a instalar la aplicación bajo estudio se pueda traducir en una medida arbitraria, irrazonable o desproporcionada. Recuérdese que, según lo expuesto, la medida se tomó por motivos de seguridad institucional y, además, no representa ninguna amenaza o violación a la intimidad y privacidad del funcionario (al desacreditarse el acceso a sus datos personales).
De todos modos, conviene aclararle al tutelado que, en caso de considerar que fue sancionado en calidad de funcionario público y no se respetó, al efecto, el debido proceso, debe acudir ante la jurisdicción laboral a formular el reclamo que considere pertinente. En ese particular, en la Sentencia No. 2025-3678 de las 09:20 hrs. de 7 de febrero de 2025 este Sala dispuso lo siguiente:
"(…) cuando quien recurre ante la Sala Constitucional para atacar presuntas violaciones al debido proceso constitucional, es funcionario o servidor público, como ocurre en este caso, debe hacérsele saber que en lo tocante a supuestos quebrantos sustanciales al debido proceso en la función pública, los servidores afectados deben acudir ante la jurisdicción laboral, toda vez que, ante la promulgación de la Reforma Procesal Laboral, Ley N° 9343 de 25 de enero de 2016 —que está vigente desde el 25 de julio de 2017—, esta Sala, en sentencia N° 2017-017948 de las 9:15 horas del 8 de noviembre de 2017, indicó lo siguiente: "(…) Ciertamente, la tutela de la Sala Constitucional, en tratándose de la materia laboral, deriva de la aplicación del Título V, Capítulo Único, de la Constitución Política, denominado Derechos y Garantías Sociales. Es allí, donde encuentran protección constitucional, por medio del recurso de amparo, el derecho al trabajo, al salario mínimo, a la jornada laboral, al descanso semanal, a vacaciones anuales remuneradas, a la libre sindicalización, al derecho de huelga, a la celebración de convenciones colectivas de trabajo, entre otros; todo ello, con ocasión del trabajo. Sin embargo, bajo una nueva ponderación, dada la promulgación de la Reforma Procesal Laboral, Ley N° 9343 de 25 de enero de 2016, vigente desde el 25 de julio de 2017, esta Sala considera que ahora todos los reclamos relacionados con esos derechos laborales, derivados de un fuero especial (por razones de edad, etnia, sexo, religión, raza, orientación sexual, estado civil, opinión política, ascendencia nacional, origen social, filiación, discapacidad, afiliación sindical, situación económica, así como cualquier otra causal discriminatoria contraria a la dignidad humana), tienen un cauce procesal expedito y célere, por medio de un proceso sumarísimo y una jurisdicción plenaria y universal, para su correcto conocimiento y resolución, en procura de una adecuada protección de esos derechos y situaciones jurídicas sustanciales, con asidero en el ordenamiento jurídico infra constitucional, que tiene una relación indirecta con los derechos fundamentales y el Derecho de la Constitución. Iguales razones caben aplicar para las personas servidoras del Estado, respecto del procedimiento ante el Tribunal de Servicio Civil que les garantiza el ordenamiento jurídico, así como las demás personas trabajadoras del Sector Público para la tutela del debido proceso o fueros semejantes a que tengan derecho de acuerdo con el ordenamiento constitucional o legal. En fin, el proceso sumarísimo será de aplicación, tanto del sector público como del privado, en virtud de un fuero especial, con goce de estabilidad en el empleo o de procedimientos especiales para su tutela, con motivo del despido o de cualquier otra medida disciplinaria o discriminatoria, por violación de fueros especiales de protección o de procedimientos, autorizaciones y formalidades a que tienen derecho, las mujeres en estado de embarazo o periodo de lactancia, las personas trabajadoras adolescentes, las personas cubiertas por el artículo 367, del Código de Trabajo, las personas denunciantes de hostigamiento sexual, las personas trabajadoras indicadas en el artículo 620, y en fin, de quienes gocen de algún fuero semejante mediante ley, normas especiales o instrumentos colectivos de trabajo. Esta nueva legislación incorpora, en el ordenamiento jurídico, una serie de novedosos mecanismos procesales: como plazos más cortos para la realización de los actos procesales, una tutela jurisdiccional más eficaz, asistencia legal gratuita, implementa la oralidad en los procedimientos; y, como consecuencia, incluye los sub-principios de concentración, inmediación y celeridad, tasa de forma expresa las situaciones en las que cabe ejercer los medios de impugnación, entre otros institutos, todo lo cual tiende a la realización de una eficaz tutela judicial en materia laboral, como garantía de protección de los derechos laborales constitucionales, dadas las nuevas características de simplicidad, celeridad y prontitud de los procesos laborales, lo que constituye una mayor garantía para la efectiva protección de las situaciones jurídicas sustanciales que involucren aspectos laborales y en las que, para su debida tutela, se requiera recabar elementos probatorios o zanjar cuestiones de mera legalidad. De modo, que las pretensiones deducidas en este recurso de amparo, son propias de ser conocidas a través de los nuevos mecanismos procesales que prevé la citada Reforma Procesal Laboral o, en su caso, ante la jurisdicción de lo contencioso administrativo, de conformidad con lo resuelto por esta Sala en la Sentencia N° 2008-002545 de las 8:55 horas del 22 de febrero de 2008, motivo por el cual, lo procedente es rechazar de plano el recurso y remitir a la parte interesada a la jurisdicción competente, para que sea allí donde reciba, en forma plena, la tutela judicial que pretende (…)".

F. Teletrabajo como herramienta opcional para el recurrente. Finalmente, es importante tomar en cuenta –tal y como

informó la autoridad recurrida– que la implementación del doble factor de autenticación en el dispositivo móvil propiedad de un funcionario de la SUTEL no es una obligación impuesta ni obstaculiza su trabajo, sino que es una medida de seguridad que deben implementar, únicamente, si desean laborar en la modalidad de teletrabajo. En ese sentido, es claro que, si no desean instalar la herramienta en análisis en sus dispositivos móviles, los funcionarios (como es el caso del recurrente), tienen la posibilidad de realizar sus labores de forma presencial en las oficinas de la SUTEL.

***

Bajo dicha inteligencia, al descartarse quebranto alguno a los derechos fundamentales del recurrente, lo que procede es desestimar el presente proceso de amparo. (…)"

... Ver menos

Texto de la Resolución

□□□□□□□□□□□□□□□□□□

Exp: 25-024824-0007-CO
Res. Nº 2025032917

SALA CONSTITUCIONAL DE LA CORTE SUPREMA DE JUSTICIA. San José, a las nueve horas veinte minutos del diez de octubre de dos mil veinticinco .

Recurso de amparo interpuesto por [Nombre 001], cédula de identidad [Valor 001], contra **LA SUPERINTENDENCIA DE TELECOMUNICACIONES (SUTEL).**

RESULTANDO:

1.- Por escrito aportado a la Sala el 19 de agosto de 2025, el recurrente interpone recurso de amparo y manifiesta que labora para la Superintendencia de Telecomunicaciones como Jefe de la Dirección General de Calidad. Preliminarmente, aduce que acude a la Sala por violación a su derecho a la intimidad y a la autodeterminación informativa (artículo 24 de la Constitución Política), "*por la obligación impuesta por parte de la institución para acceder a mi teléfono móvil personal con el fin de instalar de una aplicación (sic) de autenticación de segundo factor para acceso y uso remoto del equipo, correo electrónico, programas institucionales y red privada virtual".* Explica que mediante el proceso de licitación No. 2023LE-000002-0014900001, la autoridad recurrida promovió una contratación para efectos de atender las disposiciones contenidas en la Directriz No. 133-MP-MICITT del 21 de abril del 2022 y demás normativa en materia de seguridad informática. Mediante oficio No. 01718-SUTEL-CS-2025 de 27 de febrero de 2025, el Consejo de SUTEL consultó a la Jefatura de Unidad de Tecnologías de Información de esa entidad sobre la posibilidad de utilizar tokens físicos como mecanismo de doble factor de autenticación. Lo anterior en el tanto, en la licitación promovida y adjudicada por la SUTEL, se estableció como requisito obligatorio la compatibilidad de la herramienta WatchGuard con dicho tipo de dispositivos. Mediante oficio No. 02006-SUTEL-DGC-2025 de 5 de marzo de 2025, la Jefatura de la Unidad de Tecnología de Información de la SUTEL concluyó que el licenciamiento adquirido permite agregar tokens físicos, no requiere de un software adicional y que el objetivo de no utilizar tokens físicos responde a un interés institucional de evitar una erogación de fondos adicionales por parte de la superintendencia. Explica que, en su lugar, se optó por instalar en los teléfonos móviles personales de los funcionarios la aplicación AuthPoint de WatchGuard en el tanto "*los funcionarios que cuentan con la modalidad de teletrabajo han utilizado su dispositivo móvil personal para el uso de las herramientas de Microsoft 365 como correo electrónico y teams, así como Microsoft Authenticator desde el año 2022*." Asimismo, en el citado oficio se señaló cuáles son los funcionarios que, a la fecha, no habían instalado la aplicación WatchGuard en sus teléfonos móviles personales. Apunta que, mediante correo electrónico, se comunicó el acuerdo No. 005-042-2025 de la sesión ordinaria de 31 de julio de 2025, el cual otorgó un plazo de cinco días hábiles (a partir de la notificación), a los funcionarios que no contaban con la aplicación de doble factor de autenticación (2FA) en sus dispositivos móviles para la instalación de dicha herramienta. Es decir, el Consejo de SUTEL otorgó carácter obligatorio a la aplicación de doble factor de autenticación en los teléfonos móviles personales de los funcionarios de la institución para lo cual, incluso, estableció un plazo de cumplimiento de esta disposición. Refiere que, mediante oficio No. 07175-SUTEL-SCS-2025 de 1° de agosto de 2025, el Consejo de SUTEL comunicó a la totalidad de funcionarios de la entidad una serie de disposiciones con respecto al asunto del doble factor de autenticación en computadoras institucionales. Entre los aspectos comunicados se indicó lo siguiente: "*3. INSTRUIR a la Unidad de TI coordinar la configuración el doble factor de autenticación (2FA) en la VPN a todos los funcionarios de la SUTEL. 4. INDICAR a todos los funcionarios que no está autorizado el uso de computadoras personales o equipos que no sean los institucionales para acceder a cualquier plataforma institucional, así como, tampoco está autorizado la instalación de VPN sin contar con los controles mínimos de seguridad establecidos en los parámetros técnicos definidos por el MICITT. 5. INSTRUIR a la Unidad de Tecnologías de Información (TI), para que en conjunto con la Unidad de Recursos Humanos (RRHH), realice el abordaje a los funcionarios que aún no tienen el doble factor de autenticación, para que se propicie su instalación, en el plazo establecido en el punto 6. 6. OTORGAR un plazo de 5 días hábiles a partir de la notificación de este acuerdo a los funcionarios que no cuentan con la instalación de la aplicación del doble factor de autenticación (2FA) en sus dispositivos móviles para la instalación de esa herramienta, lo cual deberán coordinar con la Unidad de TI".* Asimismo, en el citado oficio se le comunicó a todo el personal de la SUTEL cuáles eran los funcionarios que aún no contaban con el doble factor de autenticación en sus teléfonos personales, así como los motivos por los cuáles se encontraba pendiente la instalación de manera individualizada para cada empleado. Apunta que, en respuesta a la anterior disposición, mediante oficio No. 07246-SUTEL-DGC-2025 de 4 de agosto de 2025, varios funcionarios (entre ellos su persona), solicitaron la instalación del doble factor de autenticación (2FA) en un dispositivo móvil

personal de tipo token físico del mismo fabricante de la aplicación de autenticación elegida por la institución, el cual fue adquirido a un representante autorizado. Lo anterior en concordancia con lo señalado por la Unidad de Tecnología de Información de SUTEL mediante oficio No. 02006-SUTEL-DGC-2025 de 5 de marzo de 2025, según el cual el licenciamiento adquirido por la Superintendencia permite agregar tokens físicos, por lo que su aprovisionamiento es completamente posible. Refiere que mediante oficio No. 07255-SUTEL-DGO-2025 de 4 de agosto de 2025, la Jefatura de la Unidad de Tecnologías de Información convocó a varios funcionarios de SUTEL a las instalaciones de la entidad con el fin de proceder a la instalación obligatoria del doble factor de autenticación en los teléfonos móviles personales de los funcionarios. Aduce que la actuación de SUTEL se puede considerar como una invasión al ámbito privado personal e, incluso, familiar de los funcionarios, en el tanto requiere acceso a su teléfono personal para efectos de instalar una aplicación sobre la cual se desconoce el alcance de sus funciones y la interacción que podría tener con otras aplicaciones y datos personales del funcionario que se encuentran en su móvil. Sostiene que la instalación forzosa en un dispositivo personal tiende a habilitar accesos técnicos (permisos del sistema, lectura de metadatos, geolocalización, lista de contactos, uso de cámara/micrófono, etc.) o controles que afectan la esfera privada y familiar. Alega que cualquier injerencia sobre la documentación privada y comunicaciones requiere de una habilitación por medio de legislación especial o bien, orden de una autoridad judicial competente en la cual se establezca con claridad el control estricto de fines, medios y alcance; aspectos desconocidos por los funcionarios actualmente y sobre los cuales la institución ha omitido pronunciarse. Sostiene que la instalación de una aplicación en un dispositivo móvil personal de un funcionario podría permitir el acceso a datos e información vinculada a este dispositivo tales como geolocalización, desplazamientos e, incluso, en algunos casos, datos relacionados con la salud y la condición física del titular del teléfono, información que registra el dispositivo móvil personal en la mayoría de los casos y que constituye información personal que se encuentra tutelada por el ámbito de intimidad y privacidad de las personas. Indica que, a la fecha, el Consejo de SUTEL, así como la Unidad de Tecnologías de Información, han sido omisos en identificar con claridad los alcances de la instalación de la aplicación descrita en los teléfonos celulares personales de los funcionarios. Por lo anterior, a la fecha se desconoce si esta aplicación interactúa con otras funciones de los teléfonos celulares personales de los funcionarios, en cuyo caso debe requerirse el otorgamiento de un consentimiento para su instalación. Para estos efectos se debe contar con la información suficiente y necesaria sobre los datos que eventualmente podrían estar siendo compartidos con la institución una vez instalada la aplicación. Agrega que el artículo 24 de la Constitución Política garantiza el derecho a la intimidad, la inviolabilidad de documentos privados y el secreto de las comunicaciones, por lo que cualquier injerencia en estos ámbitos debe contar con una habilitación legal expresa y someterse a control judicial. La obligación de instalar una aplicación en un dispositivo personal en el cual se cuenta con datos y funciones privadas vulnera directamente estos derechos, en particular si se desconoce el alcance de la aplicación y su interacción con otras funcionalidades de los teléfonos celulares personales. En caso de que la aplicación que se pretende instalar de manera obligatoria en los teléfonos de los funcionarios de la institución permita el acceso a la revisión, almacenamiento, registro o bloqueo de comunicaciones (incluidas notificaciones) en el dispositivo, se roza la intervención de comunicaciones en los términos previstos por el artículo 24 de la Constitución Política. Por otra parte, el derecho a la autodeterminación informativa, derivado del citado artículo 24 y reconocido como derecho fundamental autónomo por la Sala Constitucional, exige que el tratamiento de datos personales se realice con consentimiento libre, informado y expreso, el cual no existe si la instalación es impuesta como condición laboral. Menciona que existe una asimetría en la información que maneja la administración y los funcionarios a los cuales se les exige instalar una aplicación en el teléfono móvil personal. Esto hace que no se cuente, por parte de los funcionarios a los que se pretende instalar la aplicación, con el detalle del alcance y las funciones de la misma y, en su lugar, únicamente se ha gestionado de forma insistente por el Área de Tecnologías de Información y Comunicación de la institución su instalación obligatoria en los teléfonos de los funcionarios. Lo anterior resulta contrario al principio de autodeterminación informativa tutelado por la Constitución y sobre el cual se ha pronunciado la Sala Constitucional. Agrega que la SUTEL ha insistido en instalar una aplicación en los teléfonos celulares personales de los funcionarios de la institución y concomitantemente se ha negado a utilizar otros medios de factor de doble autenticación incluso, los que se encuentran dentro del ámbito de la contratación realizada por la entidad para estos fines y a la disposición manifestada por los funcionarios de asumir el costo de mecanismos sustitutos a la instalación de la aplicación como sería el uso de token físicos. Indica que, para evidenciar la perseverancia de la SUTEL en imponer la instalación de la aplicación en cuestión, comunicó a la totalidad del personal y expuso de forma arbitraria los nombres de los funcionarios que se oponen a la medida, señalando las consecuencias a las cuales se exponían por ese motivo, lo cual se traduce en una especie de sanción moral. Indica que se trató de una medida unilateral, coercitiva, sorpresiva e innecesaria para los funcionarios afectados, a quienes se les expuso y se les dejó sin posibilidad de ejercer el derecho a la defensa y emitir su posición. Incluso, en dicho oficio no se expuso el argumento por el cual algunos funcionarios como su persona se oponen a la decisión del Consejo de la Unidad de Tecnologías de Información de la SUTEL. Sostiene que su posición no es antojadiza ni responde a un capricho, sino que pretende que se garantice el respeto a la privacidad y a la intimidad de quienes se oponen a dicha medida. Agrega que el Consejo de SUTEL no ha emitido un pronunciamiento expreso sobre los motivos por los cuales no se considera su propuesta. En virtud de lo anterior, estima lesionado lo dispuesto en el ordinal 24 constitucional. Solicita que se declare con lugar el recurso y se le ordene al Consejo de la SUTEL "*dejar sin efecto la disposición relacionada con la instalación de una aplicación únicamente en los teléfonos celulares personales de sus funcionarios por ser contraria a las disposiciones constitucionales señaladas".*

2.- Por resolución de las 12:07 hrs. de 26 de agosto de 2025, se le da curso al proceso y se requieren los informes a las autoridades recurridas.

3.- Mediante memorial aportado a la Sala el 2 de septiembre de 2025, Federico Chacón Loaiza, en su condición de Presidente del Consejo y representante judicial y extrajudicial de la Superintendencia de Telecomunicaciones, rinde informe y señala expresamente lo siguiente: *"(…) 1. ANTECEDENTES A continuación, se realiza mención de los hechos de interés para el presente asunto, todo lo cual se aporta como prueba adjunta. A. El 21 de agosto del 2024, el Consejo de Sutel celebró la sesión ordinaria 036-2024, en la cual adoptó el acuerdo no. 018-036-2024, que en lo relevante dispuso: "(...) 3. SOLICITAR a la Unidad de Tecnologías de Información que coordine y promueva con los usuarios que no instalaron el método de doble factor de autenticación en sus computadoras institucionales, que lo instalen como parte de las medidas de seguridad que ha solicitado el MICITT. En caso*

de que persista la imposibilidad de su implementación por negativa de los funcionarios, la Unidad de Tecnología de Información deberá coordinar y junto con la Unidad Jurídica, resolver lo que en derecho corresponda y en su caso, proponer las acciones respectivas o establecer los mecanismos o medidas para hacer exigible a todos los funcionarios el método de doble factor de autenticación en las computadoras institucionales para lo cual es necesario el uso de los dispositivos celulares de los funcionarios (...)." B. El 25 de setiembre el 2024, el Consejo de Sutel celebró la sesión ordinaria 046-2024 en la cual se adoptó el acuerdo no. 014-046-2024, que en lo relevante dispuso: " 1. Dar por recibido el oficio OF-0025-AFAS-2024 mediante el cual la Asociación de Funcionarios ARESEP-SUTEL, consulta la posición del Consejo con respecto a la instalación del doble factor de autenticación en el dispositivo móvil personal de los funcionarios de la SUTEL. 2. Trasladar el oficio mencionado en el numeral 1 a la Unidad Jurídica y a la Unidad de Tecnologías de la Información para su atención." C. El 04 de noviembre de 2024 en el oficio 09751-SUTEL-DGO-2024, la Jefatura de la Unidad Jurídica y la Jefatura de la Unidad de Tecnologías de Información de la Sutel, emitió criterio técnico-jurídico sobre el doble factor de autenticación como requerimiento para que los funcionares de dicha institución apliquen la modalidad de teletrabajo, en atención a los acuerdos 018-036-2024 y 014-046-2024 de referencia y, recomendó al Consejo de la Sutel lo siguiente: "1. Dar por recibido y acoger en su totalidad, lo indicado en el oficio 09367-SUTELDGO-2024, emitido por la Unidad de Tecnologías de Información y la Unidad Jurídica de la SUTEL. 2. Dar por atendida la instrucción realizada en el punto 2 del acuerdo no. 014-046- 2024 adoptado en la sesión ordinaria 046-2024 del Consejo de la Superintendencia de Telecomunicaciones, celebrada el 25 de setiembre del 2024, que dispuso la remisión a la Unidad Jurídica y a la Unidad de Tecnologías de la Información, el oficio F-0025-AFAS-2024 de la Asociación de funcionarios Aresep y Sutel. 3. Instruir a la Dirección General de Operaciones para que la Unidad de Recursos Humanos contando con la asesoría de la Unidad Jurídica, proponga ante el Consejo, las gestiones necesarias para documentar y garantizar la implementación de las herramientas que ha escogido la institución, para prevenir ataques cibernéticos y garantizar el resguardo, protección e integridad de los datos y equipos propiedad de la institución, incluyendo el factor de doble autenticación. 4. Instruir a la Unidad de Tecnologías de Información, para que remita el punto 1 del apartado V del oficio de criterio técnico y jurídico no. 09367-SUTEL-DGO-2024, en respuesta del oficio No. 07763-SUTEL-DGC-2024, emitido por colaboradores de la Dirección General de Calidad. 5. Instruir a la Secretaría del Consejo, para notifique el punto 2 del apartado V a la Asociación de funcionarios Aresep y Sutel, como respuesta a la consulta notificada mediante el oficio no. F-0025-AFAS-2024. 6. Instruir a la Unidad de Comunicación para que divulgue la guía del uso de aplicativo de doble factor de autenticación para los usuarios y el protocolo de atención en caso de incidente al momento de autenticar al usuario en la computadora, correo, herramientas colaborativas o VPN, el cual deberá ser proporcionado por la Unidad de TI. 7. Instruir a Recursos Humanos para que solicite a las jefaturas de las Unidades, la lista de las personas que se oponen a la implementación del doble factor de autenticación para validar con el Consejo, las medidas a adoptar. 8. Instruir a Recursos Humanos para que una vez que cuente con la lista de los funcionarios que no desean implementar el doble factor de autenticación le proporcione a la Unidad de TI esa lista, con el fin de que TI realice la actualización correspondiente al MICITT e indique los métodos que utilizará en las oficinas centrales para mitigar los riesgos asociados a la no utilización del método instruido por el MICITT." D. El 20 de febrero del 2025, mediante oficio 01480-SUTEL-UJ-2025, la Unidad Jurídica de la Sutel brindó respuestas a las consultas efectuada por el Consejo de la Sutel mediante oficio 01076-SUTEL-CS-2025, en relación con el doble factor de autenticación como requerimiento para que los funcionares de dicha institución apliquen la modalidad de teletrabajo. E. El 6 de marzo del 2025, en oficio 02006-SUTEL-DGC-2025, el Jefe de la Unidad de Tecnologías de Información de la Sutel brindó respuestas a las consultas efectuada por el Consejo de la Sutel mediante oficio 01718-SUTEL-CS-2025, en relación con el doble factor de autenticación como requerimiento para que los funcionares de dicha institución apliquen la modalidad de teletrabajo. F. El 19 de junio del 2025, circular MIDEPLAN-DM-CIRC-0004-2025-MICITT-DM-CIREC008-2025 del 19 de junio de 2025 las ministras de Planificación Nacional y Política Económica y Ciencias, Innovación, Tecnología y Telecomunicaciones emitieron la siguiente instrucción a los jerarcas institucionales: "Así las cosas, y con sustento legal en el principio de seguridad de la información y en protección del funcionamiento institucional, desde el Ministerio de Planificación Nacional y Política Económica (MIDEPLAN), en su rol como ente rector del Sistema General de Empleo Público, se instruye a la institucionalidad pública centralizada y recomienda a las instituciones descentralizadas la suspensión del beneficio de teletrabajo para todo el personal, hasta en tanto se subsanen los faltantes técnicos aquí señalados relativos a el acceso mediante red privada virtual (VPN) con autenticación multifactor (2FA) y restricción geográfica para permitir conexiones solo de acceso desde Costa Rica; además de acceso correo electrónico mediante autenticación multifactor (2FA). Para esto se deberá velar por la aplicación de la norma N° 9738, Ley Para Regular el Teletrabajo. Adicionalmente, se recuerda que no está autorizado el uso de computadoras personales o equipos que no sean institucionales para acceder a cualquier plataforma institucional, así como tampoco la instalación de VPN sin contar con los controles mínimos de seguridad establecidos en los parámetros técnicos definidos por el MICITT. Una vez implementados los mecanismos de seguridad según lo referido por el MICITT, se podrá restablecer el beneficio de teletrabajo, conforme a los lineamientos vigentes. Adicionalmente, se deberá informar a la Dirección de Ciberseguridad al correo electrónico direccion.ciberseguridad@micitt.go.cr a fin de actualizar el estado de la institución en cuanto a la aplicación de las medidas básicas de ciberseguridad." (Destacado intencional) G. El 31 de julio del 2025, el Consejo de la Sutel celebró la sesión ordinaria 042-2025, en la cual adoptó el acuerdo 005-042-2025, que en lo relevante dispuso lo siguiente: " (…) 1. DAR por recibido y acoger el oficio 06676-SUTEL-UJ-2025, emitido por la Unidad de TI en conjunto con la Unidad Jurídica y tener por atendido lo dispuesto en el punto 2 del acuerdo 014-035-2025 emitido por el Consejo de SUTEL. 2. DAR POR RECIBIDO el oficio MICITT-DM-OF-869-2025 del 11 de julio de 2025 (NI-09403-2025). 3. INSTRUIR a la Unidad de TI coordinar la configuración el doble factor de autenticación (2FA) en la VPN a todos los funcionarios de la SUTEL. 4. INDICAR a todos los funcionarios que no está autorizado el uso de computadoras personales o equipos que no sean los institucionales para acceder a cualquier plataforma institucional, así como, tampoco está autorizado la instalación de VPN sin contar con los controles mínimos de seguridad establecidos en los parámetros técnicos definidos por el MICITT. 5. INSTRUIR a la Unidad de Tecnologías de Información (TI), para que en conjunto con la Unidad de Recursos Humanos (RRHH), realice el abordaje a los funcionarios que aún no tienen el doble factor de autenticación, para que se propicie su instalación, en el plazo establecido en el punto 6. 6. OTORGAR un plazo de 5 días hábiles a partir de la notificación de este acuerdo a los funcionarios que no cuentan con la instalación de la aplicación del doble factor de autenticación (2FA) en sus

dispositivos móviles para la instalación de esa herramienta, lo cual deberán coordinar con la Unidad de TI. 7. SOLICITAR a la Unidad de TI que envíe un reporte al Consejo de los funcionarios que no atendieron el punto 6 de este acuerdo para proceder con la REVOCACIÓN inmediata del contrato de teletrabajo, según lo establece el artículo 9 inciso b) del Reglamento de teletrabajo en la Autoridad Reguladora de los servicios públicos y su órgano desconcentrado (Reglamento de teletrabajo) 8. AUTORIZAR al Presidente del Consejo a dar respuesta al oficio MICITT-DMOF-869- 2025 del 11 de julio de 2025 (NI-09403-2025) en el cual se le debe informar al MICITT el estado de aplicación de las medidas básicas de seguridad." H. El 06 de agosto del 2025, el recurrente y otros funcionarios de la Sutel mediante oficio 07358-SUTEL-DGC-2025 presentaron recurso de reconsideración y solicitud de medida cautelar contra el acuerdo 005-042-2025, en el cual solicitaron: "(…) Con base en lo expuesto, solicitamos respetuosamente al Consejo de la Sutel: 1. Admitir el presente recurso de reconsideración contra el acuerdo número 005- 042-2025 para su trámite y resolución. 2. Acoger la medida cautelar solicitada, suspendiendo los efectos del acuerdo número 005- 042-2025 y los oficios 07255-SUTEL-DGO-2025 y 07275-SUTELDGO-2025 hasta la resolución del presente recurso de reconsideración. 3. Aclarar que la autenticación mediante tokens físicos permite cumplir con las disposiciones de la circular MIDEPLAN-DM-CIRC-004-2025 - MICITT-DM-CIRC2025 ya que el MICITT no define un método en específico por lo que la SUTEL puede disponer de una solución de seguridad que brinde el MFA en diferentes condiciones (Físico, token OTP, etc). 4. Ordenar a la Unidad de Tecnologías de la Información que permita y habilite la utilización del doble factor de autenticación mediante dispositivos tipo token físico, sea que estos sean adquiridos por parte de la institución, o bien, mediante el aporte voluntario de los funcionarios, siempre y cuando se cumpla con los estándares de compatibilidad que la herramienta exige según el principio de neutralidad tecnológica." I. El 07 de agosto del 2025, el recurrente y otros funcionarios de la Sutel mediante oficio 07374-SUTEL-DGC-2025 presentaron una ampliación del recurso de reconsideración, sobre la correcta interpretación y aplicación de la circular MIDEPLANDM-CIRC-004-2025- MICITT-DM-CIRC-2025, referente al uso de dispositivos de segundo factor de autenticación (2FA), en la cual solicitaron: " (…) 1. Admitir la presente adenda al recurso de reconsideración interpuesto contra el acuerdo número 005-042-2025 para su trámite y resolución. 2. Acoger la medida cautelar solicitada, suspendiendo los efectos del acuerdo número 005-042-2025 y los oficios 07255-SUTEL-DGO-2025 y 07275-SUTELDGO-2025 hasta la resolución del presente recurso de reconsideración 3. Aclarar que la autenticación mediante tokens físicos indistintamente de su propiedad (adquiridos por los funcionarios o por la institución) permite cumplir con las disposiciones de la circular MIDEPLAN-DM-CIRC-004-2025 - MICITT-DMCIRC-2025 ya que el MICITT no define un método en específico por lo que la SUTEL puede disponer de una solución de seguridad que brinde el MFA en diferentes condiciones (Físico, token OTP, etc). 4. Ordenar a la Unidad de Tecnologías de la Información que permita y habilite la utilización del doble factor de autenticación mediante dispositivos tipo token físico, sea que estos sean adquiridos por parte de la institución, o bien, mediante el aporte voluntario de los funcionarios, siempre y cuando se cumpla con los estándares de compatibilidad que la herramienta exige según el principio de neutralidad tecnológica." J. El 14 de agosto de 2025 por medio del oficio 07673-SUTEL-UJ-2025 la Unidad Jurídica emitió criterio jurídico en relación con el recurso de reconsideración presentado por el recurrente y otros funcionarios de la Sutel, criterio que fue acogido en su totalidad en la resolución RCS-188-2025, adoptada por el Consejo de la Sutel en el acuerdo 007-046- 2025 del 21 de agosto del 2025, donde se resolvió el recurso de reconsideración planteado por el aquí recurrente y otros funcionarios de la Sutel contra el acuerdo 005- 042-2025, en los siguientes términos: "1. DECLARAR SIN LUGAR, el recurso de reconsideración interpuesto por los funcionarios de la Dirección General de Calidad en contra del acuerdo 005-042- 2025 del 01 de agosto del 2025. 2. RECHAZAR la medida cautelar solicitada en contra del 005-042-2025 del 01 de agosto del 2025." K. El Director de Ciberseguridad del MICITT, vía correo electrónico del 31 de agosto del 2025, señaló lo siguiente ante una consulta del Sutel: "Agradezco el contexto remitido respecto al uso de autenticación multifactor (MFA) y, en particular, la integración de WatchGuard AuthPoint adquirida mediante la contratación 2023LE-000002-001490001. Como criterio técnico y en coherencia con la Directriz MICITT-DGDCFD-DRII-AT-082-2024, reitero que cada institución, por medio de su departamento de TI, es la responsable de valorar el riesgo, definir e implementar las soluciones de seguridad que correspondan a su realidad operativa, siempre que cumplan los controles mínimos establecidos. Ello obedece a que los recursos presupuestarios, el personal y los factores técnicos son conocidos en detalle por la jefatura de TI, quien es la autoridad técnica y el máximo responsable de la gestión, configuración y correcta implementación de las plataformas y controles de seguridad. Cuando existe una compra institucional vigente como la señalada, su despliegue demuestra el debido cuidado y la debida diligencia (due care/due diligence) para proteger el acceso a servicios críticos (PC, VPN, correo, entre otros) mediante el control 2FA definido por el departamento responsable. En ese escenario corresponde hacer uso eficiente de los recursos ya invertidos y operar el control conforme al marco contractual y a las mejores prácticas, incluidos los procesos de soporte, mantenimiento y niveles de servicio provistos por el adjudicatario. La directriz no prescribe marcas ni impone un único método de MFA; exige controles efectivos. Si el análisis técnico y de costo-beneficio de la Unidad de TI determinó que la verificación por notificación push de AuthPoint es la opción adecuada para integrar con el perímetro y la VPN institucional, y dicha configuración cumple los mínimos exigidos (registro seguro del segundo factor, protección contra suplantación, trazabilidad, revocación oportuna y soporte), el enfoque es válido. Respecto de los tokens físicos, no están excluidos per se, siempre que su uso se gestione bajo administración institucional y por medio de procesos de contratación que aseguren soporte, ciclo de vida, inventario y cumplimiento. En cambio, incorporar tokens adquiridos a título personal, fuera de la contratación vigente, no es recomendable por los riesgos y vacíos de control que introduce. Entre los riesgos adicionales que deben considerarse se encuentran la ausencia de SLA y garantías del proveedor y del ciclo de vida del segundo factor (altas, bajas, revocación inmediata ante cambios o pérdidas); afectaciones a la continuidad operativa si no existen métodos de respaldo (TOTP/FIDO2), cuentas de emergencia controladas y pruebas periódicas; riesgos en la cadena de suministro al adquirir dispositivos por canales no verificados; y compromisos de interoperabilidad y experiencia de usuario que deben balancearse sin sacrificar controles. Por lo cual, se recomienda que todo control debe ser valorado de previo por el departamento responsable en este caso el departamento de informática, responsable de brindar soporte a los elementos tecnológicos de la institución. En términos operativos, resulta conveniente normar en un documento institucional los métodos MFA permitidos (Política de Control de acceso), ya que esto puede abrir puertas para que el personal no informático, tome decisiones cuál método desea y no el que la institución defina. Asimismo, corresponde recordar que el departamento de informática es el administrador del contrato y el responsable del soporte del bien adquirido en la 2023LE-000002-

001490001, debiendo velar porque el control funcione conforme a lo contratado o, en su caso, escalar y exigir el soporte que está previsto en dicha contratación. En contraste, una adquisición que no forme parte del bien institucional y por la cual el departamento de TI no sea responsable, puede constituir un riesgo operativo, legal y de sostenibilidad del control por carecer de cobertura formal de soporte y gobierno. A la luz de la circular MIDEPLA-DM-CIRC-004-2025-MICITT-DM-2025, mis respuestas no excluyen métodos específicos ya que el MICITT es agnósticos a las soluciones de seguridad y respetuoso de los procesos de cada institución que conocen su contexto y recursos. Por lo cual el MICITT requiere que se garantice la aplicación del control de seguridad que minimicen los riesgos de seguridad en estos vectores; enfatiza la responsabilidad del departamento de TI de seleccionar e instrumentar el mecanismo de MFA que resulte idóneo para su contexto, cumpliendo los mínimos exigidos por la directriz y aprovechando los recursos institucionales en este caso la contratación institucional vigente. Por estas razones, la incorporación de tokens personales fuera del marco contractual no se recomienda. Respetando el marco de competencias y lo señalado, se recomienda que la Unidad de TI, como autoridad técnica, valore el riesgo y defina el mecanismo de MFA adecuado, asegurando el cumplimiento de la directriz del MICITT y su gestión conforme a los instrumentos legales pertinentes." L. El recurrente y otros funcionarios solicitaron al Consejo de la Sutel, a la Unidad Jurídica y a la Unidad de Tecnología de Información una reunión, la cual fue programada para el 1 de setiembre del 2025, pero fue cancelada por el mismo recurrente el viernes 29 de setiembre del 2025. M. A la fecha, el señor [Nombre 001] es el único funcionario de la Sutel que se opone a instalar el doble factor de autenticación en su dispositivo móvil como requisito para efectuar el teletrabajo. 2. JUSTIFICACIÓN TÉCNICA Y JURÍDICA DEL DOBLE FACTOR DE AUTENTICACIÓN (2FA) EN LOS DISPOSITIVOS MÓVILES DE LOS FUNCIONARIOS DE LA SUTEL PARA REALIZAR TELETRABAJO Con el fin de realizar una comprensión de la medida adoptada por la Sutel, relacionada con el requerimiento del doble factor de autenticación en los dispositivos móviles de los funcionaros de dicha institución para que, apliquen la modalidad de teletrabajo, se debe partir de que existen políticas públicas que se deben acatar en materia de ciberseguridad. Al respecto, se debe mencionar en primer lugar, la directriz 133-MP-MICITT: "DIRIGIDA A LA ADMINISTRACIÓN PÚBLICA CENTRAL Y DESCENTRALIZADA SOBRE LAS MEJORAS EN MATERIA DE CIBERSEGURIDAD PARA EL SECTOR PÚBLICO DEL ESTADO", en la cual el Gobierno de la República designó al Ministerio de Ciencia, Telecomunicaciones y Tecnología (en adelante MICITT) como el ente rector de la ciberseguridad en el país, y al cual le corresponde determinar las directrices en materia de ciberseguridad para todas las instituciones públicas del Estado y, sus órganos desconcentrados. Además, el MICITT como ente rector de ciberseguridad en el país, emitió los siguientes oficios: ▪ MICITT-DC-CSIRT-AT-0319-2024, el cual indica lo siguiente: "Utilice la autenticación multifactor (MFA): imponga el uso de la MFA para acceder a sistemas críticos y datos confidenciales. La MFA agrega una capa adicional de seguridad, lo que dificulta que los atacantes obtengan acceso no autorizado." ▪ MICITT-DC-CSIRT-AT-233-2024, el cual, en la sección de recomendaciones, indica: "Autenticación multifactor (MFA): aplique la MFA, especialmente en todas las aplicaciones y servicios de acceso remoto, incluidos el correo web o el correo electrónico basado en la nube. Se debe considerar la protección adicional para las cuentas o la infraestructura críticas, incluidos los controladores de dominio." ▪ MICITT-DGDCFD-DRII-AT-082-2024, el cual indica lo siguiente: "Se recomienda aplicar la autenticación multifactor (MFA) en todas las aplicaciones y servicios de acceso remoto. Esto proporciona una capa adicional de Seguridad al requerir que los usuarios proporcionen múltiples formas de autenticación, como una contraseña y un código de verificación enviado a su dispositivo móvil. Esto dificulta que los atacantes puedan acceder a las cuentas incluso si obtienen las credenciales de inicio de sesión". ▪ Por último, el 19 de junio del 2025, mediante circular MIDEPLAN-DM-CIRC-0004-2025- MICITT-DM-CIREC-008-2025 del 19 de junio de 2025, las ministras de Planificación Nacional y Política Económica y Ciencias, Innovación, Tecnología y Telecomunicaciones emitieron la siguiente instrucción a los jerarcas institucionales: "Así las cosas, y con sustento legal en el principio de seguridad de la información y en protección del funcionamiento institucional, desde el Ministerio de Planificación Nacional y Política Económica (MIDEPLAN), en su rol como ente rector del Sistema General de Empleo Público, se instruye a la institucionalidad pública centralizada y recomienda a las instituciones descentralizadas la suspensión del beneficio de teletrabajo para todo el personal, hasta en tanto se subsanen los faltantes técnicos aquí señalados relativos a el acceso mediante red privada virtual (VPN) con autenticación multifactor (2FA) y restricción geográfica para permitir conexiones solo de acceso desde Costa Rica; además de acceso correo electrónico mediante autenticación multifactor (2FA). Para esto se deberá velar por la aplicación de la norma N° 9738, Ley Para Regular el Teletrabajo. Adicionalmente, se recuerda que no está autorizado el uso de computadoras personales o equipos que no sean institucionales para acceder a cualquier plataforma institucional, así como tampoco la instalación de VPN sin contar con los controles mínimos de seguridad establecidos en los parámetros técnicos definidos por el MICITT. Una vez implementados los mecanismos de seguridad según lo referido por el MICITT, se podrá restablecer el beneficio de teletrabajo, conforme a los lineamientos vigentes. Adicionalmente, se deberá informar a la Dirección de Ciberseguridad al correo electrónico direccion.ciberseguridad@micitt.go.cr a fin de actualizar el estado de la institución en cuanto a la aplicación de las medidas básicas de ciberseguridad." (Destacado intencional) (Ver prueba adjunta) De modo tal que existen políticas públicas de ciberseguridad dirigidas a todas las instituciones públicas del país, según las cuales el beneficio de teletrabajo debe contar con los requerimientos técnicos relativos al acceso mediante red privada virtual (VPN) con autenticación multifactor (2FA) y restricción geográfica para permitir conexiones solo de acceso desde Costa Rica; además de acceso correo electrónico mediante autenticación multifactor (2FA). Cabe recalcar que el no implementar el método de doble factor de autenticación (2FA) representa un riesgo crítico para la seguridad de la información en cualquier organización. Confiar únicamente en contraseñas expone a los sistemas institucionales a ataques comunes como el phishing, el robo de credenciales, o el uso de contraseñas reutilizadas, facilitando accesos no autorizados a información sensible, servicios críticos o recursos internos. Este tipo de brechas puede derivar en pérdida de información confidencial, continuidad operativa, daño reputacional e incluso sanciones regulatorias, especialmente en el sector de gobierno como lo es SUTEL. La implementación de 2FA mitiga significativamente estos riesgos al requerir una segunda forma de verificación mediante una aplicación autenticadora. Esto bloquea vectores de ataque como el robo de contraseñas, los intentos de fuerza bruta, y los accesos indebidos incluso si las credenciales han sido comprometidas. Adoptar 2FA es una de las medidas más efectivas y de bajo costo para fortalecer la postura de ciberseguridad y proteger tanto a los usuarios como a la organización. Asimismo que, como ya se ha mencionado en múltiples informes técnicos, la elección de Watchguard Authpoint que fue adquirido por SUTEL mediante la contratación 2023LE-000002- 001490001 para la implementación de 2FA en SUTEL busca la consolidación de un único método de

doble factor de autenticación para los procesos de inicio de sesión en los equipos portátiles, conexión remota a la red interna por medio de VPN y acceso al correo y herramientas colaborativas del office 365 institucional. En consonancia con lo expuesto, en el oficio 09751-SUTEL-DGO-2024 del 4 de noviembre del 2024, la Jefatura de la Unidad Jurídica y la Jefatura de la Unidad de Tecnologías de Información de la Sutel, emitieron criterio técnico-jurídico sobre el doble factor de autenticación como requerimiento para laborar, únicamente, en la modalidad de trabajo, en donde se señaló, para lo que interesa, lo siguiente: " III. CRITERIO TÉCNICO DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN DE SUTEL SOBRE LA IMPLEMENTACIÓN DEL FACTOR DE DOBLE AUTENTICACIÓN (…) 1. IMPORTANCIA DE LA IMPLEMENTACIÓN DEL MULTI FACTOR DE AUTENTICACIÓN (MFA) Es necesario explicar la importancia del uso de una herramienta para contar con multi factor de autenticación de los usuarios, principalmente, en un contexto de teletrabajo. En ese sentido, el doble factor de autenticación 2FA o MFA, es una medida de seguridad crucial en cualquier organización, especialmente, en las entidades gubernamentales, donde la protección de datos sensibles y la integridad de los sistemas es fundamental para evitar amenazas cibernéticas. Implementar 2FA ofrece una capa adicional de protección, haciendo que sea significativamente más difícil para los atacantes, comprometer cuentas o acceder a información confidencial de la entidad. El objetivo principal de esta herramienta es identificar que, los funcionarios de la institución son quienes verdaderamente está solicitando acceso o conexión a los sistemas, desde la conexión a la computadora institucional, acceso remoto mediante la VPN (Virtual Private Network), acceso a su correo electrónico y herramientas de colaboración, evitando así, el acceso a los sistemas y bases de datos institucionales. (…) 4. DE LA HERRAMIENTA CONTRATADA MEDIANTE EL PROCEDIMIENTO DE CONTRATACIÓN NO. 2023LE-000002-00149000 B. DE LAS CARACTERÍSTICAS DE LA HERRAMIENTA Es importante recalcar que, la herramienta utiliza como método de autenticación, el dispositivo móvil, celular o smartphone, mediante la aplicación Authpoint y que, se utiliza, exclusivamente, para que el usuario valide su identidad al acceder a los sistemas. Mediante una sola aplicación, se puede validar el acceso a la computadora, a las herramientas colaborativas de Microsoft, como Teams y Outlook y, por último, la VPN. Adicionalmente, se debe aclarar que la herramienta no tiene las siguientes funcionalidades: determinar la ubicación del dispositivo, realizar una intrusión en el sistema operativo del dispositivo móvil donde se instala u obtener información privada del funcionario, es únicamente, un método para verificar la identidad del funcionario. (…) C. DEL CUMPLIMIENTO DE LAS HERRAMIENTAS DE CIBERSEGURIDAD PARA REALIZAR TELETRABAJO Las herramientas de doble factor de autenticación, se consideran una condición mínima tecnológica, con la que, debe contar la persona teletrabajadora, lo que implica una medida de seguridad informática. Por lo tanto, dentro de las competencias de la Unidad de Tecnologías de Información, está la de definir las condiciones mínimas, con el apoyo del Consejo de la Sutel, para establecer las directrices relacionadas con el tema de ciberseguridad, lo cual ha sido reconocido y establecido en el acuerdo no. 018-036-2024. Con respecto a la referencia del uso de dispositivos celulares personales, es indispensable señalar que, bajo la línea de criterio incluido en las consultas, si los funcionarios no cuentan con disponibilidad para instalar el MFA, siendo consecuentes con esa postura, la Unidad de TI, no instalaría otras aplicaciones institucionales en esos dispositivos, exceptuando el caso de la herramienta de autenticación dispuesta por el fabricante de las licencias ofimáticas institucionales que todos los funcionarios ya tienen instalada. (…) IV. DEL CRITERIO LEGAL EN RELACIÓN CON LA IMPLEMENTACION DEL FACTOR DE DOBLE AUTENTICACIÓN EN DISPOSITIVOS MÓVILES" "Como se ha expuesto, en la Sutel, casi la totalidad de los colaboradores tienen un contrato de teletrabajo. Por lo que, para poder tener esa modalidad (teletrabajo), deben cumplir una serie de requisitos que establece el Reglamento de teletrabajo en la Autoridad Reguladora de los servicios públicos y su órgano desconcentrado (Reglamento de teletrabajo), tanto en aspectos de salud ocupacional, como, en aspectos de tecnologías de información. En caso de no cumplir con esos requisitos, no se puede suscribir el contrato de teletrabajo. (…) 1. DE LA OBLIGACIÓN DE APLICAR LAS HERRAMIENTAS DE CIBERSEGURIDAD Los colaboradores de la SUTEL que se encuentran en la modalidad de teletrabajo tienen la obligación de cumplir con los requisitos que establece el Reglamento de teletrabajo en la Autoridad Reguladora de los servicios públicos y su órgano desconcentrado (Reglamento de teletrabajo). Como se expuso, y en atención a los ataques cibernéticos que han sufrido varias instituciones públicas, se han emitido decretos y directrices que obligan a todas las instituciones y a sus funcionarios, a implementar medidas de ciberseguridad. La herramienta escogida por la Sutel tiene como objetivo: el resguardo, la protección e integridad de los datos y equipos propiedad de la institución. Por lo que, los colaboradores de la Sutel están en la obligación de aplicar las herramientas de ciberseguridad que ha escogido la institución, para prevenir este tipo de ataques. Esta herramienta cumple con el interés institucional de resguardar la seguridad de los sistemas, datos, equipos e información de la SUTEL y, con la necesidad de la implementación de medidas de seguridad. Es una herramienta avalada por la Unidad de Tecnologías de Información que es el órgano competente para emitir este tipo de recomendaciones. El Reglamento de Teletrabajo, contempla la obligación de los colaboradores de la Sutel, de usar las herramientas para resguardar la protección e integridad de los datos y equipos propiedad de la institución, como lo es, el doble factor de autenticación. Por lo expuesto, el requisito de aplicar la herramienta de ciberseguridad determinada por la institución es otra condición técnica que deben cumplir los colaboradores que realizan teletrabajo. C. ANÁLISIS DE RAZONABILIDAD EN LA IMPLEMENTACIÓN DEL FACTOR DE DOBLE AUTENTICACIÓN Es procedente analizar el uso de la herramienta de doble autenticación, a la luz de criterios de razonabilidad y, así, respaldar si esta medida es proporcional y razonable, considerando los siguientes aspectos. a. Fin lícito Es fundamental que la medida de doble autenticación persiga un fin lícito. En este caso, el objetivo es fortalecer la seguridad de la información y proteger los datos sensibles y equipos de la SUTEL. Asimismo, el fin de la herramienta de seguridad indicada, se deriva de las diversas directrices emitidas por el MICITT y el criterio técnico de la Unidad de Tecnologías de Información de la SUTEL, considerando la competencia de esta última área que se deriva del RIOF y del Reglamento de teletrabajo que aplica a la entidad. b. Análisis fáctico La implementación de la herramienta de doble autenticación a través de dispositivos móviles resulta ser una medida razonable y proporcional. No solo busca un fin lícito relacionado con la protección de datos, sino que también, se fundamenta en principios de necesidad, adecuación y proporcionalidad que son fundamentales en el marco jurídico costarricense. Esto asegura que la medida adoptada por la institución pública esté alineada con los derechos y obligaciones de los funcionarios en modalidad de teletrabajo, así como, con la necesidad de protección de los datos y sistemas de la entidad. VII. CONCLUSIONES De acuerdo con lo antes expuesto, se concluye lo siguiente: 1. La Unidad Jurídica determina que: A- Los colaboradores de la SUTEL que se encuentran en la modalidad de teletrabajo tienen la obligación de cumplir con los requisitos que establece el Reglamento de teletrabajo en la Autoridad Reguladora de los servicios públicos y su órgano

desconcentrado (Reglamento de teletrabajo), en relación con las condiciones vigentes establecidas por tecnologías de información y salud ocupacional (artículo 6). B- Los colaboradores de la Sutel están en la obligación de aplicar las herramientas de ciberseguridad que ha escogido la institución, para prevenir ataques cibernéticos y garantizar el resguardo, protección e integridad de los datos y equipos propiedad de la institución (artículos 6 y 10 Reglamento de teletrabajo). C- El requisito de aplicar la herramienta de ciberseguridad determinada por la institución es otra condición técnica que deben cumplir los colaboradores que realizan teletrabajo (artículos 6 y 10 Reglamento de teletrabajo). D- La instalación del doble factor de autenticación en dispositivos móviles propiedad de funcionarios de SUTEL, es un requisito técnico ligado a la modalidad de teletrabajo, a la que acceden de manera voluntaria los colaboradores de SUTEL. E- El Reglamento de Teletrabajo contempla la obligación de los funcionarios de tramitar una adenda al contrato de teletrabajo en caso de que varíe alguna de las condiciones, como el cambio en las condiciones mínimas de tecnologías de información (artículo 12 Reglamento de teletrabajo). F- La implementación de la herramienta de doble autenticación a través de dispositivos móviles resulta ser una medida razonable y proporcional que, logra un equilibrio entre la seguridad de la información y el respeto a los derechos individuales de los funcionarios, al circunscribirse el uso de la herramienta, a la voluntariedad de decidir si acceden a la modalidad de teletrabajo, sin dejar de lado, la importancia de que los datos, sistemas, equipos de la SUTEL se adquieren mediante fondos públicos que se deben salvaguardar, fiscalizar y proteger 2. Del análisis realizado, la Unidad de TI determina que: A- la instalación del doble factor de autenticación en dispositivos móviles, aunque no es la única forma técnicamente viable para cumplir con este método de autenticación, es la opción que por temas de eficiencia, costo y versatilidad para el usuario final recomienda sea ha utilizado por los funcionarios que se encuentran en la modalidad de teletrabajo, con el fin de mitigar los riesgos ante el uso únicamente lo cual ha demostrado ser un método insuficiente en una era disruptiva de ciberataques, donde esas contraseñas constantemente se ven comprometidas a través de la ingeniería social, ataques de fuerza bruta, suplantación de identidad (phishing), hurto por medio de algoritmos de inteligencia artificial para el uso de estas en la deep y dark web y en un entorno descentralizado como es el que se presenta en los funcionarios en teletrabajo que se encuentran fuera del anillo de protección institucional y deben conectarse desde diferentes fuentes y destinos hacia los sistemas institucionales de la SUTEL. La aplicación del método de doble factor de autenticación le permite a la institución cumplir con las normas regulatorias en materia de ciberseguridad tanto en el ámbito nacional como los estándares internacionales expuestos en este documento. B- En el caso de que algún funcionario que en la modalidad de teletrabajo no desee implementar la medida del doble factor de autenticación, la Unidad de TI cuenta con los métodos de seguridad alternativos que permiten prescindir de este método, aplicables dentro de un entorno centralizado y controlado por medio de verificaciones físicas a través de la red local y la trazabilidad de la autenticación de los usuarios en las oficinas centrales de la institución donde el funcionario deberá realizar su jornada laboral de manera presencial. A pesar de esto, aun cuando el funcionario no requiera doble factor de autenticación para acceder a los sistemas institucionales o a la computadora personal designada por la SUTEL, deberá conservar el método de doble factor de autenticación de las herramientas colaborativas y ofimática, lo cual es parte de los requisitos mínimos solicitados por el fabricante. (…)" De lo expuesto anteriormente, se deduce que la Unidad de Tecnologías de Información - unidad competente para "elaborar el conjunto de estándares, normas y procedimientos en materia de tecnologías de información y comunicación para la adquisición, el uso y administración de los bienes y servicios informáticos", según el artículo 50 inciso 3) del Reglamento interno de organización y funciones de la Autoridad Reguladora de los Servicios Públicos y su órgano desconcentrado-, emitió el criterio técnico que justifica la implementación de la herramienta denominada WatchGuard Authpoint en los dispositivos móviles personales de los funcionarios, como requisito para realizar el doble factor de autenticación y permitir a los funcionarios laborar en la modalidad de teletrabajo. De dicho criterio técnico, se extrae que el requerimiento en análisis tiene como objetivo principal velar por el interés público, al fortalecer la seguridad de la información y proteger los datos sensibles y equipos de la Sutel ante las continuas violaciones y hackeos de información que se han dado a nivel nacional. Asimismo, la implementación de la herramienta de seguridad indicada se deriva de las diversas directrices y lineamientos emitidos por el MICITT y el MIDEPLAN, que, provienen de marcos regulatorios que rigen a todas las instituciones públicas. Es importante recalcar que, tal y como se indicó en el oficio 09751-SUTEL-DGO-2024, la herramienta elegida utiliza como método de autenticación, el dispositivo móvil, celular o smartphone, mediante la aplicación AuthPoint y que, se utiliza, exclusivamente, para que el usuario valide su identidad al acceder a los sistemas. Por lo que, mediante una sola aplicación, se puede validar el acceso a la computadora, a las herramientas colaborativas de Microsoft, como Teams y Outlook y, por último, la VPN. Ahora bien, con respecto al alegato del recurrente relacionado con que se eligió el uso de los dispositivos móviles de los funcionarios y no tokens físicos, se debe indicar lo señalado en el criterio técnico 09751-SUTEL-DGO-2024, en cuanto a que el hecho de que la solución adquirida mediante la contratación 2023LE-000002-0014900001 sea compatible con tokens físicos, no implica que el token físico sea compatible con la integración del resto de procesos de autenticación internos de la institución. En ese sentido, se debe aclarar que la solución adquirida mediante la contratación 2023LE000002-0014900001 es compatible con el uso de tokens físicos para el acceso a las computadoras; sin embargo, su principal objetivo es unificar los procesos de autenticación institucionales, incluyendo el acceso al correo electrónico, la conexión remota por VPN y el inicio de sesión en la computadora. Para lograr esta integración, se requiere el uso de la aplicación móvil, de manera que, cada vez que el usuario intente acceder a alguno de estos recursos, pueda simplemente aprobar o rechazar la solicitud según corresponda. Además, que la Sutel partió de un contexto, donde todos los usuarios tenían instalada la herramienta MS Authenticator para la validación del ingreso al correo electrónico institucional, así como se indicó en el oficio 09751-SUTEL-DGO-2024: "De acuerdo con lo antes indicado, la Unidad de TI no valoró la utilización del token físico, siendo que, la totalidad de los usuarios, en el momento de esta adquisición, ya habían adoptado e instalado, la aplicación de doble factor de autenticación de Microsoft (que no contempla dispositivo físico) para el ingreso al correo electrónico, herramientas colaborativas y de ofimática, por lo que, no había una necesidad de contemplarlo." Asimismo, es fundamental aclarar que un "token físico" es un dispositivo específico dedicado exclusivamente a la generación o entrega de códigos de autenticación (por ejemplo, un llavero o tarjeta con un generador de códigos), y no se clasifica como un dispositivo móvil en sentido general. Por otro lado, un "dispositivo móvil" como un teléfono celular es un equipo multifuncional que puede alojar diversas aplicaciones, incluyendo una herramienta institucional oficial de autenticación multifactor (MFA). Ahora en relación con el rol del teléfono móvil como medio tecnológico de identificación, si bien el teléfono móvil es de uso personal, en la era digital se ha convertido en el medio tecnológico más eficaz para comprobar la identidad en entornos

corporativos. Esto se debe a que: ▪ Permite verificar en tiempo real la identidad de un usuario vinculado autorizado. ▪ Soporta múltiples factores de autenticación (contraseña, código temporal y notificación push). Por otro lado, la aplicación elegida por la Sutel corresponde a un licenciamiento institucional con métodos de contingencia en caso de que el usuario presente problemas temporales con su dispositivo móvil smartphone. De esta manera, se evidencia que la decisión de no considerar tokens físicos responde a un análisis técnico y de adopción previa, por lo que no se trató de una decisión arbitraria como lo pretende hacer ver el recurrente. Asimismo, se consideró que el uso de esa herramienta en los dispositivos móviles es la mejor opción por temas de eficiencia, costo y versatilidad para todas las partes. Por último, se indica que la Sutel adoptó un enfoque pragmático y alineado con buenas prácticas internacionales, priorizando la seguridad de los sistemas institucionales mediante la implementación de MFA en aplicaciones oficiales y confiables, con base en la experiencia operativa y las limitaciones reales sobre el control de dispositivos personales. La ausencia de una evaluación formal de riesgos sobre los dispositivos móviles personales no implica negligencia, sino un modelo de gestión equilibrado que asigna responsabilidades tanto a la institución como a los usuarios. Se reitera que las medidas de seguridad provienen del MICITT, por lo que requieren ser acatadas como herramientas que aseguren los activos institucionales. Las razones técnicas del por qué es mejor utilizar el dispositivo móvil fueron señadas a lo largo de todos los oficios rendidos por la Unidad Jurídica y la Unidad de TI (09751-SUTEL-DGO-2024 del 4 de noviembre de 2024 y 02006- SUTEL-DGC-2025 del 6 de marzo de 2025), por lo que, no es una medida antojadiza. En ese sentido, dado que la herramienta escogida por la Sutel tiene como objetivo el resguardo, la protección e integridad de los datos y equipos propiedad de la institución, se evidencia que no corresponde a una medida arbitraria, sino a una obligación que debe cumplirse, únicamente para realizar teletrabajo, por lo que no roza con derechos fundamentales de ningún tipo, por el contrario, responde a un fin público. En todo caso, es importante considerar que la implementación del doble factor de autenticación en el dispositivo móvil propiedad del colaborador, no es una obligación impuesta a los funcionarios ni obstaculiza su trabajo, sino que es una medida de seguridad que deben implementar, únicamente, si desean laborar en la modalidad de teletrabajo. En ese sentido, si no desean instalar la herramienta en análisis en sus dispositivos móviles, tienen la posibilidad de realizar sus labores en las oficinas de la Sutel. Por último, es importante agregar lo señalado por el Director Nacional de Ciberseguridad del MICITT, vía correo electrónico del 31 de agosto del 2025, ante una consulta del Sutel: "Agradezco el contexto remitido respecto al uso de autenticación multifactor (MFA) y, en particular, la integración de WatchGuard AuthPoint adquirida mediante la contratación 2023LE-000002-001490001. Como criterio técnico y en coherencia con la Directriz MICITT-DGDCFD-DRII-AT-082-2024, reitero que cada institución, por medio de su departamento de TI, es la responsable de valorar el riesgo, definir e implementar las soluciones de seguridad que correspondan a su realidad operativa, siempre que cumplan los controles mínimos establecidos. Ello obedece a que los recursos presupuestarios, el personal y los factores técnicos son conocidos en detalle por la jefatura de TI, quien es la autoridad técnica y el máximo responsable de la gestión, configuración y correcta implementación de las plataformas y controles de seguridad. Cuando existe una compra institucional vigente como la señalada, su despliegue demuestra el debido cuidado y la debida diligencia (due care/due diligence) para proteger el acceso a servicios críticos (PC, VPN, correo, entre otros) mediante el control 2FA definido por el departamento responsable. En ese escenario corresponde hacer uso eficiente de los recursos ya invertidos y operar el control conforme al marco contractual y a las mejores prácticas, incluidos los procesos de soporte, mantenimiento y niveles de servicio provistos por el adjudicatario. La directriz no prescribe marcas ni impone un único método de MFA; exige controles efectivos. Si el análisis técnico y de costo-beneficio de la Unidad de TI determinó que la verificación por notificación push de AuthPoint es la opción adecuada para integrar con el perímetro y la VPN institucional, y dicha configuración cumple los mínimos exigidos (registro seguro del segundo factor, protección contra suplantación, trazabilidad, revocación oportuna y soporte), el enfoque es válido. Respecto de los tokens físicos, no están excluidos per se, siempre que su uso se gestione bajo administración institucional y por medio de procesos de contratación que aseguren soporte, ciclo de vida, inventario y cumplimiento. En cambio, incorporar tokens adquiridos a título personal, fuera de la contratación vigente, no es recomendable por los riesgos y vacíos de control que introduce. Entre los riesgos adicionales que deben considerarse se encuentran la ausencia de SLA y garantías del proveedor y del ciclo de vida del segundo factor (altas, bajas, revocación inmediata ante cambios o pérdidas); afectaciones a la continuidad operativa si no existen métodos de respaldo (TOTP/FIDO2), cuentas de emergencia controladas y pruebas periódicas; riesgos en la cadena de suministro al adquirir dispositivos por canales no verificados; y compromisos de interoperabilidad y experiencia de usuario que deben balancearse sin sacrificar controles. Por lo cual, se recomienda que todo control debe ser valorado de previo por el departamento responsable en este caso el departamento de informática, responsable de brindar soporte a los elementos tecnológicos de la institución. (…) Asimismo, corresponde recordar que el departamento de informática es el administrador del contrato y el responsable del soporte del bien adquirido en la 2023LE-000002- 001490001, debiendo velar porque el control funcione conforme a lo contratado o, en su caso, escalar y exigir el soporte que está previsto en dicha contratación. En contraste, una adquisición que no forme parte del bien institucional y por la cual el departamento de TI no sea responsable, puede constituir un riesgo operativo, legal y de sostenibilidad del control por carecer de cobertura formal de soporte y gobierno. A la luz de la circular MIDEPLA-DM-CIRC-004-2025-MICITT-DM-2025, mis respuestas no excluyen métodos específicos ya que el MICITT es agnósticos a las soluciones de seguridad y respetuoso de los procesos de cada institución que conocen su contexto y recursos. Por lo cual el MICITT requiere que se garantice la aplicación del control de seguridad que minimicen los riesgos de seguridad en estos vectores; enfatiza la responsabilidad del departamento de TI de seleccionar e instrumentar el mecanismo de MFA que resulte idóneo para su contexto, cumpliendo los mínimos exigidos por la directriz y aprovechando los recursos institucionales en este caso la contratación institucional vigente. Por estas razones, la incorporación de tokens personales fuera del marco contractual no se recomienda. Respetando el marco de competencias y lo señalado, se recomienda que la Unidad de TI, como autoridad técnica, valore el riesgo y defina el mecanismo de MFA adecuado, asegurando el cumplimiento de la directriz del MICITT y su gestión conforme a los instrumentos legales pertinentes." (Destacado intencional) De conformidad con lo expuesto, se deduce que es a la Unidad de Tecnologías de Información a quien le corresponde verificar que el método aplicado atiende con las directrices emitidas por el MICITT y el MIDEPLAN, siendo que la incorporación de tokens personales fuera del marco contractual no se recomienda -como lo pretende el aquí recurrente- ; lo anterior, incluso podría constituir un riesgo operativo, legal y de sostenibilidad del control por carecer de cobertura formal de soporte y de gobierno, razón por la cual lo pretendido por el recurrente debe ser denegado por la

Sala Constitucional, por tratarse de una herramienta que carece de los controles por parte de la Unidad de Tecnologías de Información de la Sutel. Aquí resulta pertinente traer a colación lo señalado por la Sala Constitucional de la Corte Suprema de Justicia, en relación con las decisiones administrativas sobre ciberseguridad en las instituciones públicas: (…) En consonancia con lo expuesto, lo relativo a los estándares de ciberseguridad en Costa Rica son aspectos técnicos propios de políticas públicas de Estado que constituyen materia de gobierno, por lo que a la Sala Constitucional únicamente le corresponde verificar que no hay violación de los derechos constitucionales, lo cual no sucede en el presente caso, tal y como se expondrá con mayor detalle en el siguiente apartado (…) , la Sala Constitucional reconoce que la decisión de suspender el teletrabajo por no contar con las herramientas necesarias institucionales para el doble factor de autenticación no es arbitraria y se fundamenta en una razón objetiva, sea la existencia de criterios técnicos que hacen necesario suspender el teletrabajo, por motivos de seguridad informática, los cuales quedaron plasmados en el presente informe. Por las razones expuestas, los argumentos del señor [Nombre 001] deben ser rechazados. 3. DERECHO A LA INTIMIDAD Y PRIVACIDAD En relación con el derecho a la intimidad, libertad y al secreto de las comunicaciones, se debe traer a colación el artículo 24 de la Constitución Política, que garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones, de cuyo contenido derivan otros derechos reconocidos en el ámbito constitucional como el derecho a la imagen, la inviolabilidad de los documentos privados y de autodeterminación informativa. Específicamente el derecho a la autodeterminación informativa comprende el derecho del individuo a estar informado sobre el procesamiento de sus datos, sobre el fin que se persigue con su acceso, así como la posibilidad de tener control sobre los datos que contiene un registro y corregirlos o eliminarlos en caso de que le cause algún perjuicio. En relación con este derecho, la Sala Constitucional ha señalado que constituye una ampliación del ámbito protector del derecho a la intimidad, que surge como respuesta a los cambios en la fluidez de la información, evolucionando a nuevas herramientas de comunicación y distribución de la información, por lo que se debe garantizar el derecho fundamental de los ciudadanos a decidir quién, cuándo, dónde y bajo qué circunstancias se puede tener contacto con sus datos (sentencia de la Sala Constitucional 910-2009 de las 13:36 horas de 23 de enero de 2009). Considerando lo antes dispuesto, se debe aclarar que la medida de seguridad de doble factor de autenticación no es un gestor de información personal ni tiene como uso técnico el análisis de información contenida en los dispositivos que lo instalen. A manera de resumen, en dicho criterio la UTI señaló que las herramientas de autenticación de doble factor (2FA) son esenciales para fortalecer la seguridad de los sistemas y proteger a la institución contra accesos no autorizados. A diferencia de las contraseñas tradicionales, que pueden ser robadas o descifradas, el 2FA añade una capa adicional de seguridad, exigiendo un segundo factor de verificación, como un código de una aplicación o un mensaje push, antes de conceder acceso. Los ciberdelincuentes emplean diversas técnicas para robar credenciales, entre ellas: ▪ Ataques de fuerza bruta: Intentos automatizados para descifrar contraseñas mediante combinaciones masivas. ▪ Phishing: Engaños a los usuarios para que revelen credenciales a través de correos electrónicos, mensajes o sitios web falsos. ▪ Keylogging: Malware que registra las pulsaciones del teclado para capturar contraseñas y otros datos sensibles. ▪ Ataques de intermediario (Man-in-the-Middle): Interceptación del tráfico entre el usuario y el servidor para robar credenciales. ▪ Credential stuffing: Uso de combinaciones de usuario y contraseña filtradas en otras plataformas para intentar acceder a nuevos servicios. Para mitigar estos riesgos, se ha implementado la aplicación WatchGuard, que establece las siguientes condiciones en dispositivos móviles: (…) De lo anterior se extrae que dicha aplicación puede ver la siguiente información del dispositivo móvil: datos técnicos del dispositivo móvil; permiso para envío de notificaciones push para conexiones con computadoras, VPN u Office 365 y; acceso a la cámara solo para la activación, mediante lectura del código QR (cabe recalcar que no pide grabación y/o fotografías del rostro del funcionario). Este permiso lo requieren la mayoría de las aplicaciones en el mercado, solo para citar las más relevantes a nivel institucional: Microsoft Authenticator y a nivel personal, Google Authenticator, Whatsapp y redes sociales en general requieren este tipo de permisos. Además, este permiso se puede quitar luego de la instalación de la herramienta si así lo desea el usuario, debido a que es requerido únicamente para la lectura del código QR que asocia la cuenta al dispositivo. Cabe agregar que la aplicación no contempla permisos de acceso a archivos, fotos, ni otros datos personales disponibles, en los dispositivos en los cuales se va a instalar. Aunado a esto, el funcionamiento descrito en la ficha técnica de la solución adquirida no incluye el acceso a datos personales, sensibles para su funcionamiento. Lo anterior, la UTI lo extrajo de la página web: https://www.watchguard.com/help/docs/helpcenter/es-xl/Content/en-US/authpoint/mobile-app_see-device-info.html y además, este criterio técnico se hizo constar en el oficio emitido por la jefatura de la Unidad de Tecnologías de Información y de la Unidad Jurídica de la Sutel, número 09751-SUTEL-DGO-2024 del 4 de noviembre de 2024 y en el oficio 01480-SUTEL-UJ-2025, emitido el 20 de febrero del 2025 por la Unidad Jurídica. Asimismo, la UTI señaló que "A pesar de estas medidas, la ciberseguridad es un campo dinámico en constante evolución. Si bien ninguna solución garantiza protección absoluta, la implementación de herramientas como el doble o múltiple factor de autenticación reduce significativamente los riesgos y fortalece la seguridad de la información institucional." Aunado a lo expuesto, en el oficio 09751-SUTEL-DGO-2024 del 4 de noviembre de 2024, ya citado, en relación con este tema, se dice lo siguiente: "Adicionalmente, se debe aclarar que la herramienta no tiene las siguientes funcionalidades: determinar la ubicación del dispositivo, realizar una intrusión en el sistema operativo del dispositivo móvil donde se instala u obtener información privada del funcionario, es únicamente, un método para verificar la identidad del funcionario." Es de importancia señalar, además, lo indicado por el proveedor Tecnova Soluciones S.A en oficio del 11 de agosto del 2025, en cuanto a las funcionalidades del factor de autenticación (2FA), para ello se extrae lo siguiente y se adjunta a este informe: "En respuesta la consulta sobre la Privacidad del Usuario mencionada en el Anexo 1 del documento RECURSO DE RECONSIDERACIÓN AL ACUERDO N°005-042-2025 DEL 31 DE JULIO DEL 2025, detallamos los siguientes puntos: 1. La Política de Privacidad de Datos de la Aplicación WatchGuard Authpoint se encuentra publicada en el siguiente sitio oficial de WatchGuard Technologies: https://www.watchguard.com/es/wgrd-trust-center/privacy-guide/authpoint La consulta de la Política de Privacidad siempre es un recurso obligatorio a la hora de presentar cualquier recurso que tenga que ver con el manejo de datos privados del usuario. 2. Watchguard Technologies cumple la polí>ca GDPR de la Unión Europea para todos sus productos, puede encontrar el enunciado en el siguiente sitio web: https://www.watchguard.com/es/wgrd-trust-center/gdpr-statement A su vez también publica un Addendum sobre el Procesamiento de Datos de Clientes: https://www.watchguard.com/es/wgrd-trust-center/watchguard-technologies-inccustomer-data-processing-addendum 3. La imagen 3 del Anexo muestra un método equivocado para obtener los permisos de acceso de la aplicación WatchGuard Authpoint o cualquier otra aplicación: (…) La forma correcta es acceder a esa misma pantalla

y seleccionar los tres puntos ubicados en la esquina superior derecha y seleccionar "Todos los permisos". Esa opción muestra la lista completa de permisos a las que tienen acceso las aplicaciones: (…) Por ejemplo, esta es la lista de permisos totales de la aplicación Microsoft Excel en el mismo smartphone, donde se evidencia el acceso a recursos como "have full network access" sin que esto signifique un riesgo de seguridad para el usuario: (…) 4. En cuanto al análisis del APK de Watchguard Authpoint, se parte de una premisa incorrecta: que la simple presencia de términos técnicos en el código de una aplicación equivale a una acción maliciosa. Este enfoque carece de rigor técnico y conduce a conclusiones erróneas y alarmistas que no se corresponden con la realidad operativa de la aplicación. Muy específicamente detallamos los siguientes puntos remitendo directamente a la Guía de Privacidad oficial de WatchGuard: a. Sobre la Geolocalización y el supuesto "rastreo": i. El análisis sugiere que la aplicación funciona como un "rastreador". Esto es categóricamente falso. La propia política de WatchGuard es explícita: la recopilación de geolocalización precisa (GPS) es opcional y requiere el consentimiento explícito del usuario. Si como usuario no se autoriza este permiso, la función simplemente no se activa. Su único fin, en caso de que una empresa decida usarla, es añadir capas de seguridad adicionales, como permitir autenticaciones solo desde una ubicación específica (por ejemplo permitir las autenticaciones solo desde Costa Rica). b. Sobre la supuesta Captura de Datos Biométricos (Huella/Rostro): i. Según lo explica la guía de privacidad lo explica sin ninguna ambigüedad en la sección "Acceso a identificación biométrica": "No obtenemos acceso a los datos biométricos en sí ni los procesamos." ii. La aplicación utiliza la interfaz segura del sistema operativo del smartphone (Android o iOS). Cuando un usuario pone su huella, el sistema operativo es el que la verifica y únicamente le envía a la app una respuesta de "sí" o "no". La huella dactilar del usuario o sus datos faciales nunca salen de su dispositivo ni son visibles para WatchGuard o para el administrador de la aplicación WatchGuard Authpoint. c. Sobre los Permisos de Cámara y Red: como indica la documentación, los permisos tienen fines justificados y limitados: i. Cámara: Se usa únicamente para que el usuario escanee el código QR al momento de registrar su dispositivo. No hay otra funcionalidad asociada. ii. Red/IP: Es indispensable. La aplicación necesita conectarse a internet para validar en tiempo real que eres tú quien intenta acceder a un servicio protegido. La IP se utiliza, como se ve en la tabla de "Fines del procesamiento", para mejorar la seguridad y detectar intentos de acceso no autorizados. iii. Términos como ip, address, Location o HttpURLConnection son extremadamente comunes en cualquier aplicación que se conecte a internet o utilice servicios de Google. Están presentes en librerías estándar de Android y Google Play Services. Encontrar 84,656 coincidencias de "Red/IP" no significa que la aplicación tenga 84,656 funciones para espiar la IP; significa que el código utiliza librerías de red estándar. Reiteramos que WatchGuard AuthPoint es una herramienta segura, confiable y transparente, diseñada exclusivamente para proteger los accesos corporativos, no para invadir la privacidad de los usuarios, y está certificada como tal." (Destacado intencional) De conformidad con lo antes expuesto, es posible concluir con meridiana claridad que el doble factor de autenticación no gestiona, regula o utiliza información sensible de quienes lo instalen, por lo que no trasgrede las garantías reguladas en el artículo 24 de la Constitución Política. Además, dicha aplicación establece las condiciones de uso, mediante las cuales los eventuales usuarios se ven debidamente informados de los accesos de la aplicación. Aquí resulta pertinente señalar que los argumentos del recurrente sobre la violación a su derecho de intimidad son meras suposiciones que no cuentan con fundamento técnico y probatorio alguno. Por el contrario, tal y como se acredita en el presente informe, la herramienta no accede a los datos personales de sus usuarios. Aquí resulta importante mencionar que la Sala Constitucional en un caso similar, consideró lo siguiente: "Ahora bien, la Sala considera que los reclamos planteados no pueden prosperar por varios motivos. La Sala destaca que el accionante plantea una situación hipotética, que dista de ser una amenaza cierta, actual e inminente contra derechos fundamentales (véase, verbigracia, la resolución nro. 2018-017621 de las 10:10 horas del 23 de octubre de 2018). Si se obviara este obstáculo procesal, el recurso tampoco encontraría acogida en la Sala, toda vez que los informes rendidos desvirtúan los planteamientos del accionante. Así, en lo que respecta al rastreo y monitoreo de las personas, se tuvo por probado que la contratación versa sobre etiquetas RFID pasivas, que no permiten trazar la trayectoria de un vehículo ni establecer la posición de un vehículo en un conjunto de lecturas sucesivas. No cuentan con un sistema de referencia de posición global. En cuanto a la información que incluiría la etiqueta RFID, se indicó que sería la misma que contiene el actualmente el marchamo físico (información que está disponible para cualquier persona que lea la calcamonía que se pega en el parabrisas del vehículo). Además, el acceso a la información de la etiqueta RFID requeriría un dispositivo especial, homologado por la SUTEL, por lo que se resguardaría del uso no autorizado." (Destacado intencional) (Sentencia Nº29772-2023 de las 9:30 horas del 17 de noviembre del 2023) De modo tal que, ante la carencia de prueba que acredite que la herramienta requerida a los funcionarios de la Sutel para ejercer el teletrabajo trasgreda derecho constitucional alguno y, por tratarse de una situación hipotética que dista de ser una amenaza cierta, actual e inminente, los argumentos del recurrente deben ser rechazados, dado que se acreditó mediante criterios técnicos que no hay invasión en la privacidad e intimidad de los usuarios de dicha herramienta. III. PETITORIA Con base en los argumentos expuestos, se solicita declarar sin lugar el presente recurso de amparo, toda vez que esta Superintendencia no ha causado ninguna lesión a derechos fundamentales del recurrente (…)".

4.- En la substanciación del proceso se han observado las prescripciones de ley.

Redacta el Magistrado **Araya García**; y,

CONSIDERANDO:

I.- OBJETO DEL RECURSO. El tutelado quien labora para la SUTEL como Jefe de la Dirección General de Calidad, señala que los jerarcas de dicha entidad obligaron a los funcionarios a instalar en sus dispositivos móviles personales la aplicación AuthPoint de WatchGuard como mecanismo de doble factor de autenticación (en lugar de hacer uso de otros medios también disponibles), para poder realizar teletrabajo. Afirma que esa disposición violenta lo dispuesto en el artículo 24 de la Constitución Política y sus derechos a la intimidad, a la inviolabilidad de documentos y al secreto de las comunicaciones.

II.- HECHOS PROBADOS. De relevancia para dirimir el presente recurso de amparo, se tienen por acreditados los siguientes:

1) Mediante el proceso de licitación No. 2023LE-000002-0014900001, SUTEL promovió una contratación para efectos de atender las disposiciones contenidas en la Directriz No. 133-MP-MICITT de 21 de abril del 2022 y demás normativa en materia de seguridad informática (ver prueba).

2) El **21 de agosto de 2024**, el Consejo de SUTEL celebró la sesión ordinaria 036-2024, en la cual adoptó el acuerdo No. 018-036-2024, que en lo relevante dispuso: *"(…) 3. SOLICITAR a la Unidad de Tecnologías de información que coordine y promueva*

con los usuarios que no instalaron el método de doble factor de autenticación en sus computadoras institucionales, que lo instalen como parte de las medidas de seguridad que ha solicitado el MICITT. En caso de que persista la imposibilidad de su implementación por negativa de los funcionarios, la Unidad de Tecnología de Información deberá coordinar y junto con la Unidad Jurídica, resolver lo que en derecho corresponda y en su caso, proponer las acciones respectivas o establecer los mecanismos o medidas para hacer exigible a todos los funcionarios el método de doble factor de autenticación en las computadoras institucionales para lo cual es necesario el uso de los dispositivos celulares de los funcionarios (...)" (ver prueba).

3) El **25 de septiembre de 2024**, el Consejo de SUTEL celebró la sesión ordinaria 046-2024 en la cual se adoptó el acuerdo No. 014-046-2024, que en lo relevante dispuso: *"(…) 1. Dar por recibido el oficio OF-0025-AFAS-2024 mediante el cual la Asociación de Funcionarios ARESEP-SUTEL, consulta la posición del Consejo con respecto a la instalación del doble factor de autenticación en el dispositivo móvil personal de los funcionarios de la SUTEL 2. Trasladar el oficio mencionado en el numeral 1 a la Unidad Jurídica y a la Unidad de Tecnologías de la Información para su atención (…)"* (ver prueba).

4) El **4 de noviembre de 2024**, por oficio No. 09751-SUTEL-DGO-2024, la Jefatura de la Unidad Jurídica y la Jefatura de la Unidad de Tecnologías de Información de SUTEL, emitieron el criterio técnico jurídico sobre el doble factor de autenticación como requerimiento para que los funcionares de dicha institución aplicaran la modalidad de teletrabajo, en atención a los acuerdos Nos 018-036-2024 y 014-046-2024 de referencia y se consignó lo siguiente

"(…) III. CRITERIO TÉCNICO DE LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN DE SUTEL SOBRE LA IMPLEMENTACIÓN DEL FACTOR DE DOBLE AUTENTICACIÓN (…) 1. IMPORTANCIA DE LA IMPLEMENTACIÓN DEL MULTI FACTOR DE AUTENTICACIÓN (MFA) Es necesario explicar la importancia del uso de una herramienta para contar con multi factor de autenticación de los usuarios, principalmente, en un contexto de teletrabajo. En ese sentido, el doble factor de autenticación 2FA o MFA, es una medida de seguridad crucial en cualquier organización, especialmente, en las entidades gubernamentales, donde la protección de datos sensibles y la integridad de los sistemas es fundamental para evitar amenazas cibernéticas. Implementar 2FA ofrece una capa adicional de protección, haciendo que sea significativamente más difícil para los atacantes, comprometer cuentas o acceder a información confidencial de la entidad. El objetivo principal de esta herramienta es identificar que, los funcionarios de la institución son quienes verdaderamente está solicitando acceso o conexión a los sistemas, desde la conexión a la computadora institucional, acceso remoto mediante la VPN (Virtual Private Network), acceso a su correo electrónico y herramientas de colaboración, evitando así, el acceso a los sistemas y bases de datos institucionales. (…) 4. DE LA HERRAMIENTA CONTRATADA MEDIANTE EL PROCEDIMIENTO DE CONTRATACIÓN NO. 2023LE-000002-00149000 B. DE LAS CARACTERÍSTICAS DE LA HERRAMIENTA Es importante recalcar que, la herramienta utiliza como método de autenticación, el dispositivo móvil, celular o smartphone, mediante la aplicación Authpoint y que, se utiliza, exclusivamente, para que el usuario valide su identidad al acceder a los sistemas. Mediante una sola aplicación, se puede validar el acceso a la computadora, a las herramientas colaborativas de Microsoft, como Teams y Outlook y, por último, la VPN. Adicionalmente, se debe aclarar que la herramienta no tiene las siguientes funcionalidades: determinar la ubicación del dispositivo, realizar una intrusión en el sistema operativo del dispositivo móvil donde se instala u obtener información privada del funcionario, es únicamente, un método para verificar la identidad del funcionario. (…) C. DEL CUMPLIMIENTO DE LAS HERRAMIENTAS DE CIBERSEGURIDAD PARA REALIZAR TELETRABAJO Las herramientas de doble factor de autenticación, se consideran una condición mínima tecnológica, con la que, debe contar la persona teletrabajadora, lo que implica una medida de seguridad informática. Por lo tanto, dentro de las competencias de la Unidad de Tecnologías de Información, está la de definir las condiciones mínimas, con el apoyo del Consejo de la Sutel, para establecer las directrices relacionadas con el tema de ciberseguridad, lo cual ha sido reconocido y establecido en el acuerdo no. 018-036-2024. Con respecto a la referencia del uso de dispositivos celulares personales, es indispensable señalar que, bajo la línea de criterio incluido en las consultas, si los funcionarios no cuentan con disponibilidad para instalar el MFA, siendo consecuentes con esa postura, la Unidad de TI, no instalaría otras aplicaciones institucionales en esos dispositivos, exceptuando el caso de la herramienta de autenticación dispuesta por el fabricante de las licencias ofimáticas institucionales que todos los funcionarios ya tienen instalada. (…) IV. DEL CRITERIO LEGAL EN RELACIÓN CON LA IMPLEMENTACION DEL FACTOR DE DOBLE AUTENTICACIÓN EN DISPOSITIVOS MÓVILES" "Como se ha expuesto, en la Sutel, casi la totalidad de los colaboradores tienen un contrato de teletrabajo. Por lo que, para poder tener esa modalidad (teletrabajo), deben cumplir una serie de requisitos que establece el Reglamento de teletrabajo en la Autoridad Reguladora de los servicios públicos y su órgano desconcentrado (Reglamento de teletrabajo), tanto en aspectos de salud ocupacional, como, en aspectos de tecnologías de información. En caso de no cumplir con esos requisitos, no se puede suscribir el contrato de teletrabajo. (…) 1. DE LA OBLIGACIÓN DE APLICAR LAS HERRAMIENTAS DE CIBERSEGURIDAD Los colaboradores de la SUTEL que se encuentran en la modalidad de teletrabajo tienen la obligación de cumplir con los requisitos que establece el Reglamento de teletrabajo en la Autoridad Reguladora de los servicios públicos y su órgano desconcentrado (Reglamento de teletrabajo). Como se expuso, y en atención a los ataques cibernéticos que han sufrido varias instituciones públicas, se han emitido decretos y directrices que obligan a todas las instituciones y a sus funcionarios, a implementar medidas de ciberseguridad. La herramienta escogida por la Sutel tiene como objetivo: el resguardo, la protección e integridad de los datos y equipos propiedad de la institución. Por lo que, los colaboradores de la Sutel están en la obligación de aplicar las herramientas de ciberseguridad que ha escogido la institución, para prevenir este tipo de ataques. Esta herramienta cumple con el interés institucional de resguardar la seguridad de los sistemas, datos, equipos e información de la SUTEL y, con la necesidad de la implementación de medidas de seguridad. Es una herramienta avalada por la Unidad de Tecnologías de Información que es el órgano competente para emitir este tipo de recomendaciones. El Reglamento de Teletrabajo, contempla la obligación de los colaboradores de la Sutel, de usar las herramientas para resguardar la protección e integridad de los datos y equipos propiedad de la institución, como lo es, el doble factor de autenticación. Por lo expuesto, el requisito de aplicar la herramienta de ciberseguridad determinada por la institución es otra condición técnica que deben cumplir los colaboradores que realizan teletrabajo. C. ANÁLISIS DE RAZONABILIDAD EN LA IMPLEMENTACIÓN DEL FACTOR DE DOBLE AUTENTICACIÓN Es procedente analizar el uso de la herramienta de doble autenticación, a la luz de criterios de razonabilidad y, así, respaldar si esta medida es proporcional y razonable, considerando los siguientes aspectos. a. Fin lícito Es fundamental que la medida de doble autenticación persiga un fin lícito. En este caso, el objetivo es fortalecer la seguridad de la información y proteger los datos

sensibles y equipos de la SUTEL. Asimismo, el fin de la herramienta de seguridad indicada, se deriva de las diversas directrices emitidas por el MICITT y el criterio técnico de la Unidad de Tecnologías de Información de la SUTEL, considerando la competencia de esta última área que se deriva del RIOF y del Reglamento de teletrabajo que aplica a la entidad. b. Análisis fáctico Como se expuso, y en atención a los ataques cibernéticos que han sufrido varias instituciones públicas, se han emitido decretos y directrices que obligan a todas las instituciones y a sus funcionarios, a implementar medidas de ciberseguridad. La herramienta escogida por la Sutel tiene como objetivo: el resguardo, la protección e integridad de los datos y equipos propiedad de la institución. Por lo que, los colaboradores de la Sutel están en la obligación de aplicar las herramientas de ciberseguridad que ha escogido la institución, para prevenir este tipo de ataques. Esta herramienta cumple con el interés institucional de resguardar la seguridad de los sistemas, datos, equipos e información de la SUTEL y, con la necesidad de la implementación de medidas de seguridad. Es una herramienta avalada por la Unidad de Tecnologías de Información que es el órgano competente para emitir este tipo de recomendaciones. El Reglamento de Teletrabajo, contempla la obligación de los colaboradores de la Sutel, de usar las herramientas para resguardar la protección e integridad de los datos y equipos propiedad de la institución, como lo es, el doble factor de autenticación. Por lo expuesto, el requisito de aplicar la herramienta de ciberseguridad determinada por la institución es otra condición técnica que deben cumplir los colaboradores que realizan teletrabajo. C. ANÁLISIS DE RAZONABILIDAD EN LA IMPLEMENTACIÓN DEL FACTOR DE DOBLE AUTENTICACIÓN Es procedente analizar el uso de la herramienta de doble autenticación, a la luz de criterios de razonabilidad y, así, respaldar si esta medida es proporcional y razonable, considerando los siguientes aspectos. a. Fin lícito Es fundamental que la medida de doble autenticación persiga un fin lícito. En este caso, el objetivo es fortalecer la seguridad de la información y proteger los datos sensibles y equipos de la SUTEL. Asimismo, el fin de la herramienta de seguridad indicada, se deriva de las diversas directrices emitidas por el MICITT y el criterio técnico de la Unidad de Tecnologías de Información de la SUTEL, considerando la competencia de esta última área que se deriva del RIOF y del Reglamento de teletrabajo que aplica a la entidad. b. Análisis fáctico individuales de los funcionarios, al circunscribirse el uso de la herramienta, a la voluntariedad de decidir si acceden a la modalidad de teletrabajo, sin dejar de lado, la importancia de que los datos, sistemas, equipos de la SUTEL se adquieren mediante fondos públicos que se deben salvaguardar, fiscalizar y proteger 2. Del análisis realizado, la Unidad de TI determina que: A- la instalación del doble factor de autenticación en dispositivos móviles, aunque no es la única forma técnicamente viable para cumplir con este método de autenticación, es la opción que por temas de eficiencia, costo y versatilidad para el usuario final recomienda sea ha utilizado por los funcionarios que se encuentran en la modalidad de teletrabajo, con el fin de mitigar los riesgos ante el uso únicamente lo cual ha demostrado ser un método insuficiente en una era disruptiva de ciberataques, donde esas contraseñas constantemente se ven comprometidas a través de la ingeniería social, ataques de fuerza bruta, suplantación de identidad (phishing), hurto por medio de algoritmos de inteligencia artificial para el uso de estas en la deep y dark web y en un entorno descentralizado como es el que se presenta en los funcionarios en teletrabajo que se encuentran fuera del anillo de protección institucional y deben conectarse desde diferentes fuentes y destinos hacia los sistemas institucionales de la SUTEL. La aplicación del método de doble factor de autenticación le permite a la institución cumplir con las normas regulatorias en materia de ciberseguridad tanto en el ámbito nacional como los estándares internacionales expuestos en este documento. B- En el caso de que algún funcionario que en la modalidad de teletrabajo no desee implementar la medida del doble factor de autenticación, la Unidad de TI cuenta con los métodos de seguridad alternativos que permiten prescindir de este método, aplicables dentro de un entorno centralizado y controlado por medio de verificaciones físicas a través de la red local y la trazabilidad de la autenticación de los usuarios en las oficinas centrales de la institución donde el funcionario deberá realizar su jornada laboral de manera presencial. A pesar de esto, aun cuando el funcionario no requiera doble factor de autenticación para acceder a los sistemas institucionales o a la computadora personal designada por la SUTEL, deberá conservar el método de doble factor de autenticación de las herramientas colaborativas y ofimática, lo cual es parte de los requisitos mínimos solicitados por el fabricante. VII. RECOMENDACIONES 1. Dar por recibido y acoger en su totalidad, lo indicado en el oficio 09367-SUTEL-DGO-2024, emitido por la Unidad de Tecnologías de Información y la Unidad Jurídica de la SUTEL. 2. Dar por atendida la instrucción realizada en el punto 2 del acuerdo no. 014-046- 2024 adoptado en la sesión ordinaria 046-2024 del Consejo de la Superintendencia de Telecomunicaciones, celebrada el 25 de setiembre del 2024, que dispuso la remisión a la Unidad Jurídica y a la Unidad de Tecnologías de la Información, el oficio F-0025-AFAS-2024 de la Asociación de funcionarios Aresep y Sutel. 3. Instruir a la Dirección General de Operaciones para que la Unidad de Recursos Humanos contando con la asesoría de la Unidad Jurídica, proponga ante el Consejo, las gestiones necesarias para documentar y garantizar la implementación de las herramientas que ha escogido la institución, para prevenir ataques cibernéticos y garantizar el resguardo, protección e integridad de los datos y equipos propiedad de la institución, incluyendo el factor de doble autenticación. 4. Instruir a la Unidad de Tecnologías de Información, para que remita el punto 1 del apartado V del oficio de criterio técnico y jurídico no. 09367-SUTEL-DGO-2024, en respuesta del oficio No. 07763-SUTEL-DGC-2024, emitido por colaboradores de la Dirección General de Calidad. 5. Instruir a la Secretaría del Consejo, para notifique el punto 2 del apartado V a la Asociación de funcionarios Aresep y Sutel, como respuesta a la consulta notificada mediante el oficio no. F-0025-AFAS-2024. 6. Instruir a la Unidad de Comunicación para que divulgue la guía del uso de aplicativo de doble factor de autenticación para los usuarios y el protocolo de atención en caso de incidente al momento de autenticar al usuario en la computadora, correo, herramientas colaborativas o VPN, el cual deberá ser proporcionado por la Unidad de TI. 7. Instruir a Recursos Humanos para que solicite a las jefaturas de las Unidades, la lista de las personas que se oponen a la implementación del doble factor de autenticación para validar con el Consejo, las medidas a adoptar. 8. Instruir a Recursos Humanos para que una vez que cuente con la lista de los funcionarios que no desean implementar el doble factor de autenticación le proporcione a la Unidad de TI esa lista, con el fin de que TI realice la actualización correspondiente al MICITT e indique los métodos que utilizará en las oficinas centrales para mitigar los riesgos asociados a la no utilización del método instruido por el MICITT (…)" (ver prueba).

5) El **20 de febrero de 2025**, mediante oficio No. 01480-SUTEL-UJ-2025, la Unidad Jurídica de la SUTEL brindó respuestas a las consultas efectuada por el Consejo de la SUTEL mediante oficio No. 01076-SUTEL-CS-2025, en relación con el doble factor de autenticación como requerimiento para que los funcionarios de dicha institución apliquen la modalidad de teletrabajo. Lo anterior, conforme los siguientes términos:

"(…) II. RESPUESTA A LAS CONSULTAS A continuaci ón, se brinda respuesta a las consultas presentadas por el Consejo de SUTEL. 1. Pregunta: "Según la Ley para Regular el Teletrabajo N°9738, el teletrabajo es voluntario tanto para el empleado como para el empleador. Dado este principio de voluntariedad: ¿Es posible establecer como requisito para acceder a esta modalidad que los funcionarios autoricen la instalación de una aplicación de doble factor de autenticación en sus teléfonos personales para el cumplimiento de condiciones de seguridad, de igual forma en que se exige la provisión de mobiliario adecuado para el cumplimiento de condiciones de salud ocupacional, o de servicios básicos y acceso a internet con un mínimo de ancho de banda por parte del teletrabajador?". La Ley para regular el teletrabajo, Ley N° 9738, aplica para la Sutel, según lo que establece el artículo 2. Por lo tanto, es aplicable lo dispuesto en el artículo 9 inciso a) que establece lo siguiente: "Artículo 9- Obligaciones de las personas teletrabajadoras. Sin perjuicio de las demás obligaciones que acuerden las partes en el contrato o adenda de teletrabajo, serán obligaciones para las personas teletrabajadoras las siguientes: a) Cumplir con los criterios de medición, evaluación y control determinados en el contrato o adenda, así como sujetarse a las políticas y los códigos de la empresa, respecto a temas de relaciones laborales, comportamiento, confidencialidad, manejo de la información y demás disposiciones aplicables." El Reglamento para regular el teletrabajo, decreto Nº 42083-MP-MTSS-MIDEPLAN-MICITT, en el artículo 6 establece los deberes de las personas teletrabajadoras y indica que las personas teletrabajadoras deben cumplir lo siguiente: b) Las demás obligaciones contenidas en el contrato o adenda de teletrabajo y la legislación costarricense. De acuerdo con esa ley y reglamento, es una obligación de las personas que teletrabajan cumplir con las políticas que emita la institución, por lo que, esas normas se deben complementar con las regulaciones emitidas por la Sutel El Reglamento de Teletrabajo en la Autoridad Reguladora de los Servicios Públicos y su órgano desconcentrado (en adelante Reglamento de Teletrabajo), el cual resulta aplicable a SUTEL, dispone en lo relevante lo siguiente: "Artículo 5.- Dependencias de apoyo de la CIT y sus funciones. Son dependencias de apoyo las que a continuación se indican y tendrán las funciones siguientes: (…) b) Tecnologías de Información, se encargará de: (…) 4) Definir, actualizar y comunicar oportunamente las condiciones mínimas de tecnologías de información y comunicación con las que debe contar la persona teletrabajadora en el centro o lugar de teletrabajo, incluidas las medidas de seguridad informática". De conformidad con el reglamento antes citado, el establecimiento de condiciones mínimas en tecnologías de información que la Unidad de Tecnología de Información (en adelante UTI) defina mediante criterio técnico para personas que, voluntariamente, desean acceder a la modalidad de teletrabajo, se encuentra contemplado en la normativa específica que aplica a la SUTEL, por lo que resulta posible. Además, se destaca que el Reglamento de Teletrabajo contempla las obligaciones del funcionario en teletrabajo y, en lo que interesa dispone lo siguiente: "Artículo 2. Alcance. El presente reglamento es de acatamiento obligatorio para todas las personas funcionarias de la Autoridad Reguladora de los Servicios Públicos y su órgano desconcentrado que voluntariamente soliciten la aprobación del teletrabajo como una modalidad de trabajo a distancia mediante el uso de medios y tecnología de la información y comunicación (…) Artículo 6. - Condiciones generales del teletrabajo. Las condiciones generales del teletrabajo son las siguientes: (…) e) Requiere el uso y cumplimiento de las condiciones mínimas vigentes establecidas por tecnologías de información y salud ocupacional en el lugar o centro de teletrabajo para acceder a la modalidad de teletrabajo. (…) Artículo 10.- Requisitos de la persona teletrabajadora. La persona funcionaria que solicite el teletrabajo deberá cumplir con cada uno de los requisitos siguientes: (…) d) Cumplir con los lineamientos específicos emitidos por la CIT y las dependencias de apoyo en materia de tecnologías de la información y comunicación y de salud ocupacional. (…) Artículo 12.- Obligaciones de la persona teletrabajadora (…) b) Tramitar una adenda al contrato de teletrabajo en caso de que varíe alguna de las condiciones que justificaron su ingreso a la modalidad de teletrabajo (lugar o centro de teletrabajo estipulado, cambio de puesto, actividades o condiciones mínimas de tecnologías de información y salud ocupacional requeridas, así como el cambio permanente en los días de teletrabajo estipulados). El teletrabajo se continuará realizando hasta que se apruebe la adenda al contrato (…)". Lo anterior implica que, una vez que se defina algún requerimiento mínimo en tecnologías de información como requisito para acceder a la modalidad de teletrabajo de parte de UTI, los colaboradores que deseen estar en dicha modalidad deben cumplir con ese requisito. Cabe mencionar que el tema en cuestión fue desarrollado en el apartado IV del oficio 09751- SUTEL-DGO-2024 del 4 de diciembre del 2024. 2. Pregunta: "El artículo 24 de la Constitución Política "garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República". En este sentido, ¿la obligación impuesta a los funcionarios de utilizar sus dispositivos personales para fines laborales de autenticación en las plataformas de uso e interés exclusivamente institucional es acorde con el artículo 24 constitucional?". Previo a atender lo consultado es importante aclarar que, el criterio 09751-SUTEL-DGO-2024 no concluye que la implementación del doble factor de autenticación sea una obligación impuesta a los funcionarios para utilizar sus dispositivos personales para fines laborales, en el tanto se detalla lo siguiente: "A lo anterior, se agrega que, la instalación del doble factor de autenticación en el dispositivo móvil propiedad del colaborador, no es para el desempeño de sus labores, es únicamente, como una medida de seguridad". (Oficio 09751-SUTEL-DGO-2024). (…) De los criterios emitidos por la Sala Constitucional y la PGR, es procedente sintetizar que las garantías reguladas en el artículo 24 de la C.P., se relacionan con derechos reconocidos en el ámbito constitucional, como el derecho a la imagen, inviolabilidad de los documentos privados y de autodeterminación informativa, esta última garantía abarca el derecho del individuo a estar informado sobre el procesamiento de sus datos. Considerando lo antes dispuesto, se debe aclarar que la medida de seguridad de doble factor de autenticación no es un gestor de información personal ni tiene como uso técnico el análisis de información contenida en los dispositivos que lo instalen, por lo que resulte importante citar la siguiente opinión remitida la UTI: "Las herramientas de autenticación de doble factor (2FA) son esenciales para fortalecer la seguridad de los sistemas y proteger a la institución contra accesos no autorizados. A diferencia de las contraseñas tradicionales, que pueden ser robadas o descifradas, el 2FA añade una capa adicional de seguridad, exigiendo un segundo factor de verificación, como un código de una aplicación o un mensaje push, antes de conceder acceso. Los ciberdelincuentes emplean diversas técnicas para robar credenciales, entre ellas: Ataques de fuerza bruta: Intentos automatizados para descifrar contraseñas mediante combinaciones masivas. Phishing: Engaños a los usuarios para que revelen credenciales a través de correos electrónicos, mensajes o sitios web falsos. Keylogging: Malware que registra las pulsaciones del teclado para capturar contraseñas y otros datos sensibles. Ataques de intermediario (Man-in-the-Middle): Interceptación del tráfico entre el usuario y el servidor para robar credenciales. Credential stuffing: Uso de combinaciones de usuario y contraseña filtradas en otras plataformas para intentar acceder a nuevos servicios.

Para mitigar estos riesgos, se ha implementado la aplicación WatchGuard, que establece las siguientes condiciones en dispositivos móviles: (…) Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico El contenido generado por IA puede ser incorrecto. Permiso para envió de notificaciones push para conexiones con computadoras, VPN u Office 365. Acceso a la cámara solo para la activación, mediante lectura del código QR. (No pide grabación y/o fotografías del rostro del funcionario) Este permiso lo requieren la mayoría de las aplicaciones en el mercado, solo para citar las más relevantes a nivel institucional: Microsoft Authenticator y a nivel personal, Google Authenticator, Whatsapp y redes sociales en general requieren este tipo de permisos. Además este permiso se puede quitar luego de la instalación de la herramienta si así lo desea el usuario, debido a que es requerido únicamente para la lectura del código QR que asocia la cuenta al dispositivo. La aplicación no contempla permisos de acceso a archivos, fotos, ni otros datos personales disponibles, en los dispositivos en los cuales se va a instalar. Además el funcionamiento descrito en la ficha técnica de la solución adquirida no incluye el acceso a datos personales, sensibles para su funcionamiento. (…) A pesar de estas medidas, la ciberseguridad es un campo dinámico en constante evolución. Si bien ninguna solución garantiza protección absoluta, la implementación de herramientas como el doble o múltiple factor de autenticación reduce significativamente los riesgos y fortalece la seguridad de la información institucional (…)". (Correo electrónico del 20 de febrero del año en curso). De conformidad con lo antes expuesto, es procedente indicar que el doble factor de autenticación no tiene como fin: gestionar, regular o utilizar información sensible de quienes lo instalen, por lo que carece de relación con aquellas garantías previstas en el artículo 24 de la C.P. Además, se destaca que la instalación de la herramienta establece las condiciones de uso, mediante las cuales los eventuales usuarios se ven debidamente informados de los accesos de la aplicación. 3. Pregunta: "¿Qué obligaciones tiene la institución en cuanto a la provisión de herramientas necesarias para el teletrabajo?". Las obligaciones de la SUTEL con respecto a la provisión de herramientas para que los funcionarios que, de manera voluntaria, deseen acceder a la modalidad de teletrabajo, son aquellas previstas en la normativa que regula el teletrabajo en la entidad (incluyendo la Ley para regular el teletrabajo y su reglamento), así como, en el Reglamento de Teletrabajo y el contrato de teletrabajo suscrito. Ahora bien, a nivel interno el Reglamento de Teletrabajo, regula lo siguiente con respeto a las herramientas que debe proporcionar la entidad: (…) Asimismo, el formato de contrato de teletrabajo utilizado por SUTEL, contempla con respecto a la provisión de herramientas de parte de la entidad, lo siguiente: (…) De conformidad con lo anterior, se resumen las obligaciones que tiene la institución en cuanto a la provisión de herramientas necesarias para el teletrabajo: • Asignar una computadora portátil con sus respectivos programas. • Facilitar la utilización de algún insumo, de conformidad con la disponibilidad de activos existentes y con fundamento en el Reglamento de Propiedad, Planta y Equipo y Activos Intangibles de la Autoridad Reguladora o cualquier otra disposición que al efecto se emita. • Herramienta de mensajería instantánea y videoconferencias proporcionada e instalada por la Unidad de Tecnologías de Información de la SUTEL. • Proveer a sus teletrabajadores, las herramientas de ofimática y accesos a los recursos tecnológicos compartidos necesarios para ejercer su labor. • La herramienta de conexión remota será preinstalada en el equipo de la persona teletrabajadora, y se le capacitará sobre la forma de utilizarla. 4. Pregunta: "El Por Tanto 3. del acuerdo de este Consejo 018-036-2024 del 21 de agosto del 2024 señala: "SOLICITAR a la Unidad de Tecnologías de Información que coordine y promueva con los usuarios que no instalaron el método de doble factor de autenticación en sus computadoras institucionales, que lo instalen como parte de las medidas de seguridad que ha solicitado el MICITT. En caso de que persista la imposibilidad de su implementación por negativa de los funcionarios, la Unidad de Tecnología de Información deberá coordinar y junto con la Unidad Jurídica, resolver lo que en derecho corresponda y en su caso, proponer las acciones respectivas o establecer los mecanismos o medidas para hacer exigible a todos los funcionarios el método de doble factor de autenticación en las computadoras institucionales para lo cual es necesario el uso de los dispositivos celulares de los funcionarios" En este sentido, ¿es proporcional y razonable la implementación del doble factor de autenticación en dispositivos personales de los funcionarios bajo el principio de voluntariedad del teletrabajo, o presenta ambigüedades que podrían generar contradicciones en su aplicación?". Para atender la consulta planteada, resulta pertinente remitir a lo dispuesto en el criterio 09751- SUTEL-DGO-2024, que en lo relevante dispuso: "C. ANÁLISIS DE RAZONABILIDAD EN LA IMPLEMENTACIÓN DEL FACTOR DE DOBLE AUTENTICACIÓN Es procedente analizar el uso de la herramienta de doble autenticación, a la luz de criterios de razonabilidad y, así, respaldar si esta medida es proporcional y razonable, considerando los siguientes aspectos. a. Fin lícito Es fundamental que la medida de doble autenticación persiga un fin lícito. En este caso, el objetivo es fortalecer la seguridad de la información y proteger los datos sensibles y equipos de la SUTEL. Asimismo, el fin de la herramienta de seguridad indicada, se deriva de las diversas directrices emitidas por el MICITT y el criterio técnico de la Unidad de Tecnologías de Información de la SUTEL, considerando la competencia de esta última área que se deriva del RIOF y del Reglamento de teletrabajo que aplica a la entidad. b. Análisis fáctico De acuerdo con la información del presente criterio y alcance de la herramienta, se deben considerar los siguientes elementos: • Necesidad: El juicio de necesidad implica evaluar si existen alternativas más rentables que permitan alcanzar el mismo objetivo con igual eficacia. La implementación de la doble autenticación mediante dispositivos móviles es una medida más efectiva considerando el criterio técnico que indicó lo siguiente: "La Unidad de TI no valoró la utilización del token físico, siendo que, la totalidad de los usuarios, en el momento de esta adquisición, ya habían adoptado e instalado, la aplicación de doble factor de autenticación de Microsoft, para el ingreso al correo electrónico, herramientas colaborativas y de ofimática, por lo que, no se consideró necesario. Lo anterior debido a que, el objetivo era consolidar en una sola aplicación, el cumplimiento obligatorio de la DIRECTRIZ N°133-MP-MICITT y cumplir con las mejores prácticas y estándares internacionales mencionados anteriormente Es importante mencionar que, con esta contratación, lo que se adquiere es el uso de las licencias, por lo que, no se podría realizar una compra de hardware (tokens físicos) ya que, no serían parte del objeto de la contratación original" • Idoneidad: La medida debe ser idónea para alcanzar el fin propuesto. En este sentido, el uso de la doble autenticación a través de dispositivos móviles se presenta como una solución adecuada para mitigar el riesgo en la vulneración de equipos, sistemas y dato de la entidad, cumpliendo con la característica de idoneidad (…) • Proporcionalidad: La proporcionalidad en sentido estricto requiere un balance entre los beneficios de la medida y, otros elementos que podrían, en apariencia, generar conflicto con la implementación requerida. La necesidad de los funcionarios en teletrabajo de utilizar un sistema de doble autenticación no modifica los términos esenciales del contrato de teletrabajo, ya que, la medida aplica para aquellos colaboradores que, de manera voluntaria aplican la modalidad de teletrabajo y, por ende, deben atender las obligaciones dispuestas en el Reglamento de Teletrabajo, según el cual, se deben cumplir los requisitos técnicos mínimos. Así, se logra un

equilibrio entre la seguridad de la información y el respeto a los derechos individuales de los funcionarios, al circunscribirse el uso de la herramienta, a la voluntariedad de decidir si acceden a la modalidad de teletrabajo, sin dejar de lado, la importancia de que los datos, sistemas, equipos de la SUTEL se adquieren mediante fondos públicos que se deben salvaguardar, fiscalizar y proteger (…)". Del examen de razonabilidad antes detallado se concluyó que, la implementación de la herramienta de doble autenticación a través de dispositivos móviles es una medida razonable, que además de buscar un fin lícito vinculado con la protección de datos, también se fundamenta en principios de necesidad, adecuación y proporcionalidad que, se deben cumplir. En respuesta a la consulta y de conformidad con lo expuesto, sí es proporcional y razonable la implementación del doble factor de autenticación en dispositivos personales de los funcionarios que realizan teletrabajo. Como se ha desarrollado, el teletrabajo es una modalidad de trabajo voluntaria y quienes soliciten esa modalidad, deben cumplir con el marco jurídico que regula el tema, por lo que, las personas que no cumplan con las disposiciones emitidas en relación con el teletrabajo no pueden usar esa modalidad. De conformidad con lo expuesto, no es contradictorio ni existe ambigüedad, exigir a las personas que deseen realizar teletrabajo cumplir con las medidas de seguridad que defina la UTI y que en el caso del factor de doble autenticación atiende lo dispuesto en la directriz no. 133-MP-MICITT y decreto ejecutivo no. 43542-MP-MICITT, ambos emitidos por el MICITT. Finalmente, destacamos que en el criterio citado (09751-SUTEL-DGO-2024), se incluye la referencia a las diversas contrataciones de entidades en Costa Rica (incluyendo la Defensoría de los Habitantes), relacionadas con la implementación del factor de doble autenticación para garantizar la protección de sus datos y sistemas. 5. Pregunta: "Bajo el modelo de teletrabajo vigente la condición sobre el uso de la aplicación de doble factor de autenticación en dispositivos personales ha sido establecida por el la Unidad de Tecnologías de la Información de la Dirección General de Operaciones, producto de la contratación de la herramienta. En ese sentido: (…)". Previo a atender las consultas remitidas, es indispensable aclarar que la implementación de la medida de seguridad de doble factor de autenticación no es producto de la contratación de dicha solución. Lo anterior, considerando que el procedimiento de contratación fue una herramienta para satisfacer la necesidad de contar con tal medida de seguridad, según lo dispuesto en la directriz emitida por el MICITT, tal como se visualiza en la justificación del expediente de contratación en SICOP: "En cumplimiento a lo indicado en el artículo 37 de la LGCP y en el artículo 5 del Reglamento interno de compras públicas de la SUTEL, se justifica la procedencia de esta contratación según lo siguiente: Se encuentra dentro del objetivo estratégico #3 denominado "Garantizar la regulación efectiva y la universalidad de los servicios con base en el recurso humano necesario, competente y comprometido, apoyados por el uso de las mejores tecnologías, la gestión por resultados y la calidad regulatoria, para procurar la transformación y eficiencia de la organización", definido en el Plan Estratégico Institucional 2023-2027 y en el programa de adquisiciones institucionales del año 2024. 01-Línea 01 Licencias de Antivirus 02- Línea 02 Licencias de Multi Factor de Autenticación Es importante indicar que La Dirección General de Operaciones, Unidad de Tecnologías de Información, verificó antes de solicitar esta compra lo siguiente: 1- Que en la SUTEL no existe una contratación actual que supla lo requerido en el objeto indicado. 2- Que el servicio requerido no se puede adquirir directamente por esta área o por cualquier otra de las que conforman la SUTEL, porque corresponden a herramientas de antivirys y multi factor de autenciación que deben obtenerse para proteger a la SUTEL ante un eventual ataque donde las perdidas pueden ser mayores a la inversión. Las herramientas solicitadas son instrumentos básicos para la protección de la información institucional y el resguardo de la operación técnica de la SUTEL. Por lo anterior, al no contar SUTEL con lo requerido mediante sus áreas ni por medio de procesos de contratación vigentes, es necesario contratar los bienes y servicios indicados por medio de este procedimiento, ya que esta área requiere de ello para poder obtener herramientas de ciberseguridad licenciadas como bienes intangibles que permita tener visibilidad y proteger a la institución de amenazas latentes, en cumplimiento con el DECRETO EJECUTIVO DE EMERGENCIA N°43542-MP MICITT y en alineamiento con la Estrategia Nacional de Ciberseguridad de Costa Rica 2023-2027 del Ministerio de Ciencia, Tecnología y Telecomunicaciones. Adicionalmente la Contraloría General de la República mediante el oficio OF-0007-AI-2023 emitido por la Auditoría Interna de la ARESEP, realizó una serie de recomendaciones técnicas que estaríamos subsanando con la ejecución de esta contratación en el cumplimiento de las especificaciones técnicas solicitadas. Esta contratación se realiza nuevamente luego del resultado de la contratación 2023LY-000003-0014900001, la cual fue infructuosa para la línea relacioada (sic) con el Antivirus Institucional. La herramienta de autenticación multifactor (MFA) es fundamental para reforzar la seguridad en el acceso a sistemas y datos sensibles. Al requerir múltiples formas de verificación más allá de las contraseñas, como códigos temporales o notificaciones push, el MFA reduce el riesgo de violaciones de seguridad, protege la información confidencial y cumple con regulaciones del Código Nacional de Tecnologías Digitales Capítulo 2 Identificación y Autenticación Ciudadana. Además, en un entorno laboral remoto, garantiza un acceso seguro desde ubicaciones externas. Esta capa adicional de seguridad no solo fortalece la protección de datos, sino que también mejora la experiencia del usuario al proporcionar un acceso seguro sin comprometer la usabilidad una vez que se integra adecuadamente (…)".(Expediente en SICOP no. 2023LE-000002- 0014900001). (…) Bajo la misma línea del criterio antes citado, se atiende la consulta indicando que la implementación de las medidas de seguridad de parte de la unidad técnica competente, no obedecen a lo que indica el contrato de teletrabajo, sino que derivan de lo dispuesto en el Reglamento de teletrabajo, el cual se encuentra referenciado en el formato de contrato de teletrabajo y deben cumplir los funcionarios. Ahora bien, considerando que el Reglamento citado contempla la obligación de los colaboradores de gestionar una adenda, en caso de que cambie alguna condición mínima en tecnología, recomendamos que mediante dicha figura se incluya la herramienta dispuesta por la UTI. III. INFORMACION RELEVANTE Considerando que las consultas atendidas se relacionan con el uso de dispositivos de colaboradores para instalar la medida de seguridad del doble factor de autenticación, es de interés, compartir los siguientes datos: • "Se calcula que aproximadamente el 90% de las personas empleadas a nivel internacional utilizan de algún modo sus dispositivos para acceder a información de la organización, dado que es muy normal que dispongan de una tecnología más avanzada, productiva y eficaz que la propia organización, y que se incentiva porque además supone un gran ahorro para las organizaciones al no tener que estar destinando parte de su presupuesto de Riesgos y Seguridad de la Universidad de Costa Rica, 2022, enlace: https://ci.ucr.ac.cr/que-es-el-byod). • "El 70% de las empresas permite el acceso a los activos corporativos desde portátiles y dispositivos móviles personales Solo el 17% de las empresas limita el acceso remoto exclusivamente a los portátiles corporativos (…)". (Fuente: consulta realizada mediante Microsoft Copilot). Los datos antes referenciados, muestra el alto porcentaje de organizaciones que gestionan la utilización de dispositivos personales para acceder a información relacionada con el trabajo. Además, al igual que herramientas

personales como puede ser la silla, el escritorio y el espacio de la casa, que son necesarias para realizar el teletrabajo y son bienes personales, el dispositivo móvil de la persona trabajadora se configura como un requerimiento mínimo de carácter tecnológico para acceder al teletrabajo. Cabe resaltar que la entidad reguladora en telecomunicaciones debe buscar la eficiencia y eficacia, así como promover la tecnología necesaria para garantizar la seguridad de la información, aspecto que no resulta acorde con promover la utilización de herramientas cuya utilización se ha reducido y está en desuso y que, implican un mayor costo de fondos públicos, como lo es el token físico, con respeto a este tema, en el criterio 09751-SUTEL-DGO-2024 se indicó lo siguiente: "El objetivo y las ventajas de la implementación de la aplicación de Watchguard son las siguientes: (…) • Promueve la conveniencia y portabilidad ya que, el dispositivo móvil es algo que las personas llevan consigo todo el tiempo, lo que hace que, una app instalada en un celular, sea más accesible que llevar un token físico y, proporciona un menor riesgo de pérdida en comparación con un dispositivo físico adicional (…) • Le ahorra costos a la administración, pues no debe adquirir los tokens físicos, ya que, la app es de uso gratuito. En caso de que, no se realice el doble factor de autenticación de la manera que ha planteado la Unidad de TI, los usuarios tendrían que, utilizar una aplicación para autenticarse a las herramientas colaborativas y ofimáticas, un código proporcionado por un token físico para el login inicial en la PC y un código más, proporcionado nuevamente por el token físico, para la autenticación a la VPN, lo cual, claramente, no brinda una experiencia amigable y sencilla para el usuario final. que es una herramienta que ya no se usa porque está obsoleta, la Sutel no puede comprar herramientas obsoletas pues debemos estar a la vanguardia en las herramientas que usamos. (…) La herramienta también permite utilizar un token físico. Esta alternativa se puede evaluar (compra), siempre y cuando, se cumplan una serie de normas básicas para la seguridad de la institución y el resguardo de los activos: • El token tiene costo, por tanto, si el usuario lo pierde, se lo roban o hurtan, debe reponer el monto correspondiente para la adquisición de este. • El token debe resguardarlo de forma segura y es de uso personal e intransferible, por el periodo de tiempo que labore el funcionario en la institución. Si el funcionario renuncia o es desvinculado de la institución, SUTEL deberá iniciar las gestiones necesarias para la recuperación del token ya que sería un activo de la institución. En caso de que no se logre su recuperación, se deberá aplicar las disposiciones necesarias para gestionar el cobro del dispositivo a la persona que lo extravío para la reposición de este. La Unidad de TI no valoró la utilización del token físico, siendo que, la totalidad de los usuarios, en el momento de esta adquisición, ya habían adoptado e instalado, la aplicación de doble factor de autenticación de Microsoft, para el ingreso al correo electrónico, herramientas colaborativas y de ofimática, por lo que, no se consideró necesario. Lo anterior debido a que, el objetivo era consolidar en una sola aplicación, el cumplimiento obligatorio de la DIRECTRIZ N°133-MP-MICITT y cumplir con las mejores prácticas y estándares internacionales mencionados anteriormente. Es importante mencionar que, con esta contratación, lo que se adquiere es el uso de las licencias, por lo que, no se podría realizar una compra de hardware (tokens físicos) ya que, no serían parte del objeto de la contratación original (…)". (…)" (ver prueba).

6) Mediante oficio No. 01718-SUTEL-CS-2025 de **27 de febrero de 2025**, el Consejo de SUTEL consultó a la Jefatura de Unidad de Tecnologías de Información de esa entidad sobre la posibilidad de utilizar tokens físicos como mecanismo de doble factor de autenticación. En esta ocasión se consignó lo siguiente:

"(…) Esta Superintendencia reconoce la importancia de implementar herramientas de ciberseguridad en la institución para la protección del acervo de información que administra (bases de datos), sistemas y plataformas, razón por la cual ha implementado las políticas públicas y mecanismos tecnológicos necesarios para la protección de la información. Tal y como se desarrolla en el informe 09751-SUTEL-DGO-2024 del 4 de noviembre del 2024, es obligatorio el cumplimiento de la Directriz N°133-MP-MICITT del 21 de abril del 2022 y demás normativa en seguridad informática, el cual es y debe ser, el espíritu de las medidas de seguridad adoptadas. Por esta razón y con el fin de asegurar que las medidas de seguridad implementadas en la institución por parte de la Unidad de Tecnologías de Información son idóneas y se ajustan a los principios de transparencia, e idoneidad; este Consejo le solicita a la Unidad de Tecnologías de Información atender las siguientes consultas en un plazo de 5 días hábiles: 1. En el punto 4.4 Servicios Alternativos del documento P-PR-12.0.2 ESTUDIO MERCADO MFA del procedimiento 2023LE-000002-0014900001 (Contratación de soluciones de antivirus y multifactor de autenticación para la superintendencia de telecomunicaciones) gestionado por su Unidad se indica lo siguiente: "Para el objeto de esta contratación se identificó que existe una amplia variedad de distribuidores y/o integradores con presencial local en Costa Rica que cuentan con representaciones autorizadas de los objetos de contratación. De tal forma que siempre y cuando se cumpla con las especificaciones técnicas establecidas, son opciones que serán consideradas y serán evaluadas bajo los criterios internos establecidos." Sin embargo, no se especifica si se llevó a cabo una valoración sobre mecanismos y herramientas alternativas, cuyo análisis y descarte haya fundamentado la solución que finalmente se tradujo en los requerimientos establecidos en la línea 2 del pliego de condiciones correspondiente. En ese sentido se le solicita que desarrolle los siguientes puntos: a. De previo a la ejecución del estudio de mercado señalado ¿se evaluaron opciones como autenticación por huella digital, Microsoft Authenticator, llaves físicas USB u otros mecanismos como alternativas para el inicio de sesiones en Windows con doble factor de autenticación? b. En caso afirmativo, indique cuáles soluciones fueron inicialmente consideradas y por qué fueron finalmente descartadas en favor del mecanismo propuesto en el proceso de contratación. 2. El pliego de condiciones del procedimiento 2023LE-000002-0014900001 establece el requerimiento para que la herramienta contratada estuviese en capacidad de utilizar diferentes mecanismos de autenticación, incluyendo tokens de hardware: "12. La solución debe proporcionar al menos 3 opciones de autenticación: • Token móvil, a través de una aplicación móvil gratuita para teléfonos y tabletas con iOS y Android. • Token de hardware TOTP, fabricado por el mismo proveedor, para garantizar que los secretos del token estén siempre protegidos y nunca expuestos. • Compatibilidad con token de hardware TOTP de terceros, con claves secretas importadas mediante OATH PSKC formato (RFC 6030)" (Énfasis añadido). Por otra parte, en la sección "B. DE LAS CARACTERÍSTICAS DE LA HERRAMIENTA" del informe 09751-SUTEL-DGO-2024 del 4 de noviembre del 2024 (pg.30), se indica que: "[…] para adquirir el token físico, se requieren fondos públicos para el pago de: a- Licencia WatchGuard AuthPoint Total Identity Security b- Dispositivo en físico" (Énfasis añadido). En vista de lo anterior se le solicita aclarar lo siguiente: a. ¿El licenciamiento actual de la herramienta WatchGuard que se adquirió, permite agregar tokens físicos como mecanismo de doble factor de autenticación? b. En caso afirmativo, ¿sería necesario incorporar alguna licencia o adicionar algún elemento de software con un costo adicional? c. Como parte del proceso de recepción de la herramienta ¿se realizaron pruebas para confirmar la compatibilidad del licenciamiento actual con tokens físicos, tal como se solicitó en el pliego? 3. En la misma sección del informe se

señala que "…[n]o se identifica una necesidad ni interés público en adquirir un dispositivo token TOTP…". En este sentido, ¿qué fundamenta la inclusión de la compatibilidad con estos dispositivos como un requisito obligatorio en el pliego de condiciones para los oferentes? 4. ¿Cuáles fueron los factores considerados antes de realizar el estudio de mercado y publicar el pliego de condiciones, que llevaron a optar por no adquirir tokens físicos durante el proceso de contratación? 5. ¿Se realizó un análisis de costo-beneficio que justificara la no inclusión de tokens físicos como parte de la solución contratada? 6. ¿Se llevó a cabo una evaluación de los riesgos que podría implicar el hacer uso de dispositivos móviles personales para la autenticación en términos de seguridad u operatividad? 7. ¿Se contempló en el contrato actual la posibilidad de poder ampliar para incluir tokens físicos si posteriormente se considera necesario o en casos concretos donde no se llegase a disponer de un dispositivo móvil para la instalación de la aplicación? 8. ¿Qué procedimientos técnicos y administrativos serían necesarios para incorporar tokens de hardware al entorno actual? 9. ¿Es posible que la autenticación mediante la aplicación y mediante un token físico coexistan, permitiendo que algunos funcionarios utilicen la aplicación y otros el token físico? 10. ¿De qué forma ingresan a sus sesiones de Windows los funcionarios que aún no cuentan con la aplicación WatchGuard en sus dispositivos móviles? 11. ¿Cuántos funcionarios no cuentan con la aplicación WatchGuard en sus dispositivos móviles al momento de su respuesta? 12. ¿De parte de su Unidad se ha adoptado proactivamente alguna medida temporal específicamente dirigida a reducir el riesgo en la ciberseguridad que puede representar que algunos funcionarios no cuenten con doble factor de autenticación a la fecha? (…)" (ver prueba).

7) El **6 de marzo de 2025**, mediante oficio No. 02006-SUTEL-DGC-2025, el Jefe de la Unidad de Tecnologías de Información de la SUTEL brindó respuestas a las consultas efectuadas por el Consejo de la SUTEL mediante oficio No. 01718-SUTEL-CS-2025, en relación con el doble factor de autenticación como requerimiento para que los funcionares de dicha institución apliquen la modalidad de teletrabajo. En este oficio se consignó expresamente lo siguiente:

"(…) De conformidad con lo solicitado en el oficio 01718-SUTEL-CS-2025 la Unidad de Tecnologías de Información procede a brindar respuesta a sus consultas a continuación: 1. a: No, precisamente el estudio de mercado es el instrumento que le permite a las instituciones realizar la identificación de estándares que ofrece el mercado en cuanto a los productos y servicios disponibles con el fin de definir especificaciones técnicas realistas y ajustadas a las capacidades del mercado, tal y como lo indica el Reglamento Interno de Compra Públicas de la SUTEL en el Capítulo I, artículo 3 inciso 11 y según lo dispuesto en el artículo 34 de la LGCP que en lo relevante dispone: "(...) El estudio de mercado tendrá también como fin establecer la existencia de bienes, obras o servicios, en la cantidad, calidad y oportunidad requeridas, así como verificar la existencia de proveedores, permitir la toma de decisiones informadas respecto del procedimiento de contratación y proporcionar información para la determinación de disponibilidad presupuestaria (...)" ,por lo que la evaluación de las opciones de autenticación se realizó considerando los datos obtenidos del estudio de mercado, mismo que fue ejecutado según el debido proceso y contando con todas las aprobaciones pertinentes según lo estipulado en el proceso de contratación administrativa, tal y como consta en el expediente de la contratación 2023LE-000002-0014900001. Es importante señalar, que esta Unidad explica ampliamente las razones de porqué se elige la aplicación de WatchGuard en el oficio 09751-SUTEL-DGO-2024 en el Punto 3. HERRAMIENTAS IMPLEMENTADAS POR LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN punto C.Doble Factor de Autenticación, también se hace mención de las ventajas de utilizar un app por encima de un dispositivo físico en el Punto 4 inciso B. DE LAS CARACTERÍSTICAS DE LA HERRAMIENTA. 2. a. Sí, el licenciamiento adquirido permite agregar tokens físicos. b. No, no es requerido adicionar ningún elemento de software. c. No, ya que el criterio de la Unidad de TI determinó por conveniencia institucional y para evitar erogación de fondos adicionales a la SUTEL implementar el MFA por medio del App móvil, de conformidad con la recomendación del MICITT en el documento MICITT-DGDCFD-DRII-AT-082-2024. 3. La posibilidad de contar con algún mecanismo adicional compatible con el licenciamiento adquirido en caso de que se presentara algún incidente técnico no previsto que imposibilitara la utilización del método más económico y práctico como lo es el uso de la app móvil. 4. El criterio utilizado por la Unidad de TI se encuentra ampliamente explicado en el Punto 3. HERRAMIENTAS IMPLEMENTADAS POR LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN punto C.Doble Factor de Autenticación, también se hace mención de las ventajas de utilizar un app por encima de un dispositivo físico en el Punto 4 inciso B. DE LAS CARACTERÍSTICAS DE LA HERRAMIENTA del oficio 09751-SUTEL-DGO2024, que también es argumentado desde el punto de vista jurídico en el Punto b. Análisis fáctico del apartado C. ANÁLISIS DE RAZONABILIDAD EN LA IMPLEMENTACIÓN DEL FACTOR DE DOBLE AUTENTICACIÓN, desarrollado por la Unidad Jurídica de la SUTEL en ese mismo oficio. 5. El criterio utilizado por la Unidad de TI se encuentra ampliamente explicado en el Punto 3. HERRAMIENTAS IMPLEMENTADAS POR LA UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN punto C.Doble Factor de Autenticación, también se hace mención de las ventajas de utilizar un app por encima de un dispositivo físico en el Punto 4 inciso B. DE LAS CARACTERÍSTICAS DE LA HERRAMIENTA del oficio 09751-SUTEL-DGO-2024, que también es argumentado desde el punto de vista jurídico en el Punto b. Análisis fáctico del apartado C. ANÁLISIS DE RAZONABILIDAD EN LA IMPLEMENTACIÓN DEL FACTOR DE DOBLE AUTENTICACIÓN, desarrollado por la Unidad Jurídica de la SUTEL en ese mismo oficio. 6. No, la Unidad de TI no consideró necesario este tipo de evaluación siendo que el 100% de los funcionarios que cuentan con la modalidad de teletrabajo han utilizado su dispositivo móvil personal para el uso de las herramientas de Microsoft 365 como correo electrónico y teams, así como Microsoft Authenticator desde el año 2022. (de conformidad con las bitácoras de administración del Office 365) 7. No, tal y como se mencionó en el oficio 09751-SUTEL-DGO-2024 "(…) Es importante mencionar que, con esta contratación, lo que se adquiere es el uso de las licencias, por lo que, no se podría realizar una compra de hardware (tokens físicos) ya que, no serían parte del objeto de la contratación original." Además, según el artículo 276 del RLGCP cualquier modificación a un contrato deberá cumplir con los requisitos ahí establecidos. 8. Realizar una nueva contratación para la adquisición de tokens físicos con la debida justificación que sustente los elemento jurídicos, técnicos y financieros diferentes a los emitidos por las áreas expertas de SUTEL, cuando ya fue implementado para más del 90% de los funcionarios desde hace 8 meses una herramienta que es más rentable, eficiente y con mejores estándares de Customer Experience (CX) en caso de que se requieran, ya que como se mencionó el licenciamiento es compatible con los tokens físicos del fabricante. 9. Sí, esta información se encuentra de manera explícita en el oficio 09751-SUTEL-DGO-2024 "(…) La herramienta también permite utilizar un token físico. Esta alternativa se puede evaluar (compra), siempre y cuando, se cumplan una serie de normas básicas para la seguridad de la institución y el resguardo de los activos (…)". 10. Únicamente mediante el uso de la contraseña del equipo portátil, incumpliendo la DIRECTRIZ N°133-MP-MICITT y con esto expuestos a los posibles vectores de

ciberataques que pueden ser aprovechados por la brecha que estas vulnerabilidades presentan, poniendo en riesgo datos, información y hasta la continuidad operativa de servicios internos producto de un ataque lateral. 11. 15 funcionarios no cuentan con la aplicación WatchGuard en sus dispositivos móviles, distribuidos por área de la siguiente manera:

Dirección/Unidad	***Cantidad de funcionarios***
Consejo/Unidad Jurídica	*1*
Consejo/Unidad de Comunicación	*1*
Dirección de Mercados	*2*
Dirección de Calidd/Unidad Espectro	*2*
Dirección de Calidad/Unidad Reclamaciones	*9*

12. A modo de referencia es importante señalar que esta Unidad ha informado y gestionado oportunamente la implementación del MFA y el seguimiento al cumplimiento de las normas básicas de ciberseguridad emitidas por el MICITT siendo que el 1 de agosto del 2024, mediante el oficio 06678-SUTEL-DGO-2024 se menciona: "(…) Adicionalmente, se hace un llamado de la importancia de utilizar las herramientas de seguridad que tienen como objetivo la protección de la información de los usuarios. Se proporciona un listado de usuarios que no tienen instalado la herramienta de Multifactor de Autenticación, documento adjunto denominado: Usuarios sin MFA (…)" También, en el oficio 09751-SUTEL-DGO-2024 emitido desde el 4 de noviembre del 2024, la Unidad de TI expuso de manera detallada el criterio técnico para el cumplimiento de esta medida de seguridad, además, propuso una medida alterna para los funcionarios que no contaran con el doble factor de autenticación, sin embargo, a la fecha no ha recibido una respuesta por parte de los jerarcas de la institución con la postura oficial de la SUTEL ante el cumplimiento de la DIRECTRIZ N°133-MP-MICITT. Además, el 18 de febrero del 2025 esta Unidad emitió el oficio 01409-SUTEL-DGC-2025, donde se exponen al Director General de Operaciones con copia a los miembros del Consejo las inquietudes de la indefinición por parte de la institución ante el incumplimiento de la Directriz del MICITT y más allá de ello ante la posibilidad de la materialización de un riesgo cibernético por la no utilización del mecanismo de MFA por parte de algunos funcionarios de SUTEL, cabe destacar que estos esfuerzos se hacen en principio de buena fe por parte de esta Unidad, siendo que el Reglamento para el uso de los recursos de Tecnologías de Información de la Autoridad Reguladora de los Servicios Públicos y su órgano desconcentrado (RUTI) en el Capítulo IV El uso hardware: "Artículo 15. — Desconexión. Aquellos equipos que representen un riesgo al funcionamiento de los recursos tecnológicos de la Autoridad Reguladora serán desconectados por Tecnologías de Información sin previa comunicación al funcionario" y Capítulo V: El uso de la Infraestructura de comunicaciones: "Artículo 20. —Acceso. Para acceder a la infraestructura de comunicaciones de la Institución, los funcionarios deben identificarse por los medios establecidos para tal efecto, dicha identificación será autenticada por Tecnologías de Información antes de permitir el uso de los recursos tecnológicos. Los accesos con privilegios a los servidores se efectuarán por medio de un canal seguro dispuesto por Tecnologías de Información", faculta a la Unidad de Tecnologías de Información a tomar medidas radicales sin que medie un aviso previo. Finalmente, después de atendidas las consultas, de las cuales desde nuestro punto de vista ya habían sido abordadas ampliamente en el oficio 09751-SUTEL-DGO-2024 desde el pasado 4 de noviembre del 2024, esta Unidad sugiere que, en caso de tener aún más dudas con respecto a la utilización de los dispositivos móviles de los funcionarios para la instalación del app de MFA adquirido por la institución(y por otras instituciones como: TSE, Defensoría de los Habitantes, Poder Judicial, Asamblea Legislativa, MTSS , entre otras) , las mismas sean remitidas a la autoridad competente que corresponde al Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, quien es el ente que emite la DIRECTRIZ N°133-MP-MICITT, quien además en el documento MICITT-DGDCFD-DRII-AT-082-2024 de manera explícita en sus recomendaciones indica que el MFA utilice el dispositivo móvil de los usuarios, ya que la responsabilidad de la Unidad de TI de SUTEL únicamente es velar por el cumplimiento y el acatamiento de las directrices emitidas por este órgano gubernamental y no quien determina los métodos o herramientas que deben implementarse (…)" (ver prueba).

8) El **19 de junio de 2025**, las Ministras de Planificación Nacional y Política Económica y Ciencias, Innovación, Tecnología y Telecomunicaciones, emitieron la Circular No. MIDEPLAN-DM-CIRC-0004-2025-MICITT-DM-CIREC-008-2025, con la siguiente instrucción a los jerarcas institucionales:

"(…) Así las cosas, y con sustento legal en el principio de seguridad de la información y en protección del funcionamiento institucional, desde el Ministerio de Planificación Nacional y Política Económica (MIDEPLAN), en su rol como ente rector del Sistema General de Empleo Público, se instruye a la institucionalidad pública centralizada y recomienda a las instituciones descentralizadas la suspensión del beneficio de teletrabajo para todo el personal, hasta en tanto se subsanen los faltantes técnicos aquí señalados relativos a el acceso mediante red privada virtual (VPN) con autenticación multifactor (2FA) y restricción geográfica para permitir conexiones solo de acceso desde Costa Rica; además de acceso correo electrónico mediante autenticación multifactor (2FA). Para esto se deberá velar por la aplicación de la norma N° 9738, Ley Para Regular el Teletrabajo. Adicionalmente, se recuerda que no está autorizado el uso de computadoras personales o equipos que no sean institucionales para acceder a cualquier plataforma institucional, así como tampoco la instalación de VPN sin contar con los controles mínimos de seguridad establecidos en los parámetros técnicos definidos por el MICITT Una vez implementados los mecanismos de seguridad según lo referido por el MICITT, se podrá restablecer el beneficio de teletrabajo, conforme a los lineamientos vigentes. Adicionalmente, se deberá informar a la Dirección de Ciberseguridad al correo electrónico direccion.ciberseguridad@micitt.go.cr a fin de actualizar el estado de la institución en cuanto a la aplicación de las medidas básicas de ciberseguridad (…)" (ver prueba).

9) El **31 de julio de 2025**, el Consejo de la SUTEL celebró la sesión ordinaria No. 042-2025, mediante la cual se adoptó el acuerdo No. 005-042-2025, que dispuso lo siguiente:

"(…) 1. DAR por recibido y acoger el oficio 06676-SUTEL-UJ-2025, emitido por la Unidad de TI en conjunto con la Unidad Jurídica y tener por atendido lo dispuesto en el punto 2 del acuerdo 014-035-2025 emitido por el Consejo de SUTEL. 2. DAR POR RECIBIDO el oficio MICITT-DM-OF-869-2025 del 11 de julio de 2025 (NI-09403- 2025). 3. INSTRUIR a la Unidad de TI coordinar la configuración el doble factor de autenticación (2FA) en la VPN a todos los funcionarios de la SUTEL. 4. INDICAR a todos los funcionarios que no está autorizado el uso de computadoras personales o equipos que no sean los institucionales para acceder a

cualquier plataforma institucional, así como, tampoco está autorizado la instalación de VPN sin contar con los controles mínimos de seguridad establecidos en los parámetros técnicos definidos por el MICITT. 5. INSTRUIR a la Unidad de Tecnologías de Información (TI), para que en conjunto con la Unidad de Recursos Humanos (RRHH), realice el abordaje a los funcionarios que aún no tienen el doble factor de autenticación, para que se propicie su instalación, en el plazo establecido en el punto 6. 6. OTORGAR un plazo de 5 días hábiles a partir de la notificación de este acuerdo a los funcionarios que no cuentan con la instalación de la aplicación del doble factor de autenticación (2FA) en sus dispositivos móviles para la instalación de esa herramienta, lo cual deberán coordinar con la Unidad de TI. 7. SOLICITAR a la Unidad de TI que envíe un reporte al Consejo de los funcionarios que no atendieron el punto 6 de este acuerdo para proceder con la REVOCACIÓN inmediata del contrato de teletrabajo, según lo establece el artículo 9 inciso b) del Reglamento de teletrabajo en la Autoridad Reguladora de los servicios públicos y su órgano desconcentrado (Reglamento de teletrabajo). 8. AUTORIZAR al Presidente del Consejo a dar respuesta al oficio MICITT-DM-OF-869- 2025 del 11 de julio de 2025 (NI-09403-2025) en el cual se le debe informar al MICITT el estado de aplicación de las medidas básicas de seguridad (…)" (ver prueba).

10) Mediante oficio No. 07175-SUTEL-SCS-2025 de **1° de agosto de 2025**, el Consejo de SUTEL comunicó a los funcionarios de la entidad las anteriores disposiciones tomadas en el acuerdo No. 005-042-2025 con respecto al asunto del doble factor de autenticación en computadoras institucionales. Asimismo, en el citado oficio se le comunicó a todo el personal de la SUTEL cuáles eran los funcionarios que aún no contaban con el doble factor de autenticación en sus teléfonos personales (entre los que se encontraba el tutelado), así como los motivos por los cuales se encontraba pendiente la instalación de manera individualizada para cada funcionario (ver prueba).

11) En respuesta a la anterior disposición, mediante oficio No. 07246-SUTEL-DGC-2025 de **4 de agosto de 2025** dirigido al Consejo de la SUTEL y al Jefe de Recursos Humanos de dicha entidad, varios funcionarios (entre ellos el recurrente), solicitaron la instalación del doble factor de autenticación (2FA) en un dispositivo móvil personal de tipo token físico del mismo fabricante de la aplicación de autenticación elegida por la institución, el cual fue adquirido a un representante autorizado. Lo anterior en concordancia con lo señalado por la Unidad de Tecnología de Información de SUTEL mediante oficio No. 02006-SUTEL-DGC-2025 de marzo de 2025, según el cual el licenciamiento adquirido por la Superintendencia permite agregar tokens físicos. En tal ocasión, expresamente, los funcionarios señalaron lo siguiente:

"(…) El 1 de agosto de 2025 mediante correo electrónico se comunicó el acuerdo 005-042-2025 de la sesión ordinaria del 31 de julio de 2025 se dispuso lo siguiente: "6. OTORGAR un plazo de 5 días hábiles a partir de la notificación de este acuerdo a los funcionarios que no cuentan con la instalación de la aplicación del doble factor de autenticación (2FA) en sus dispositivos móviles para la instalación de esa herramienta, lo cual deberán coordinar con la Unidad de TI." (destacado intencional) Un token físico móvil es un pequeño dispositivo (tipo llavero electrónico) que genera códigos de acceso de un solo uso, sincronizados con la plataforma de autenticación. Su pequeño factor de forma permite movilizarlos con la persona titular. Su funcionamiento como segundo factor de autenticación es el mismo que el de las aplicaciones móviles como Authenticator de WatchGuard o Microsoft Authenticator. Sin embargo, posee la ventaja de que no es susceptible de ataques, vulneraciones de seguridad, clonación, que no requiere de acceso a Internet para funcionar y que, si se llegase a perder, no expone dato personal alguno del titular, además, su duración de batería es superior a los 7 años lo cual es superior al ciclo de vida promedio un terminal inteligente (smartphone) (…) Se les comunica que los suscritos funcionarios contamos con un dispositivo móvil personal de tipo token físico del mismo fabricante de la aplicación de autenticación elegida por la institución el cual fue adquirido a un representante autorizado: (…) [Nombre 001] (…) Se encuentra de vacaciones Como se comunicó mediante oficios número 05966-SUTEL-DGC-2025 del 1 de julio de 2025 y 05994-SUTEL-DGC-2025 del 2 de julio de 2025 estos dispositivos móviles personales de tipo token han estado disponibles desde el día de cambio de equipo institucional. Por lo tanto, se aclara que, en ningún momento, nos hemos negado al uso de un segundo factor de autenticación. Según el oficio 02006-SUTEL-DGC-2025 del 6 de marzo de 2025 el licenciamiento adquirido por la Superintendencia de Telecomunicaciones permite agregar tokens físicos por lo que su aprovisionamiento es completamente posible. Sin embargo, según lo indicado por el Sr. Alexander Herrera Céspedes, dado que en ese momento el Consejo no había autorizado el uso de dispositivos móviles personales, se nos negó su aprovisionamiento. No obstante, en la actualidad, el acuerdo 005-042-2025 del Consejo de Sutel aclaró que el método determinado por el Consejo son los dispositivos móviles personales, como el token físico, el cual ponemos a disposición. Por lo tanto, según el citado acuerdo, solicitamos que, a más tardar el martes 5 de agosto de 2025 se nos instale el segundo factor de autenticación en las computadoras institucionales que tenemos asignadas utilizando para dicho propósito nuestros dispositivos móviles de tipo token físico (…)" (ver prueba).

12) Mediante oficio No. 07255-SUTEL-DGO-2025 de **4 de agosto de 2025,** la Jefatura de la Unidad de Tecnologías de Información convocó a varios funcionarios de SUTEL (entre estos al recurrente) a las instalaciones de la entidad con el fin de proceder a la instalación del doble factor de autenticación en los teléfonos móviles personales de los funcionarios. Concretamente, dicha convocatoria se realizó para el lunes 11 de agosto de 2025 a las 08:30 hrs. en la Unidad de Tecnologías de Información (Edificio SUTEL) (ver prueba).

13) El **6 de agosto de 2025**, el recurrente y otros funcionarios de la SUTEL, mediante oficio No. 07358-SUTEL-DGC-2025, presentaron recurso de reconsideración y solicitud de medida cautelar contra el acuerdo No. 005-042-2025. En tal ocasión, solicitaron lo siguiente al Consejo de la SUTEL:

"(…) 1. Admitir el presente recurso de reconsideración contra el acuerdo número 005- 042-2025 para su trámite y resolución. 2. Acoger la medida cautelar solicitada, suspendiendo los efectos del acuerdo número 005- 042-2025 y los oficios 07255-SUTEL-DGO-2025 y 07275-SUTEL-DGO-2025 hasta la resolución del presente recurso de reconsideración. 3. Aclarar que la autenticación mediante tokens físicos permite cumplir con las disposiciones de la circular MIDEPLAN-DM-CIRC-004-2025 - MICITT-DM-CIRC-2025 ya que el MICITT no define un método en específico por lo que la SUTEL puede disponer de una solución de seguridad que brinde el MFA en diferentes condiciones (Físico, token OTP, etc). 4. Ordenar a la Unidad de Tecnologías de la Información que permita y habilite la utilización del doble factor de autenticación mediante dispositivos tipo token físico, sea que estos sean adquiridos por parte de la institución, o bien, mediante el aporte voluntario de los funcionarios, siempre y cuando se cumpla con los estándares de compatibilidad que la herramienta exige según el principio de neutralidad tecnológica (…)" (ver prueba).

14) El **7 de agosto de 2025**, el recurrente y otros funcionarios de la SUTEL, por oficio No. 07374-SUTEL-DGC-2025, presentaron ampliación del recurso de reconsideración respecto a la interpretación y aplicación de la circular No. MIDEPLANDM-CIRC-004-2025-MICITT-DM-CIRC-2025, referente al uso de dispositivos de segundo factor de autenticación (2FA), y solicitaron lo siguiente:
"(…) 1. Admitir la presente adenda al recurso de reconsideración interpuesto contra el acuerdo número 005-042-2025 para su trámite y resolución. 2. Acoger la medida cautelar solicitada, suspendiendo los efectos del acuerdo número 005- 042-2025 y los oficios 07255-SUTEL-DGO-2025 y 07275-SUTEL-DGO-2025 hasta la resolución del presente recurso de reconsideración. 3. Aclarar que la autenticación mediante tokens físicos indistintamente de su propiedad (adquiridos por los funcionarios o por la institución) permite cumplir con las disposiciones de la circular MIDEPLAN-DM-CIRC-004-2025 - MICITT-DMCIRC-2025 ya que el MICITT no define un método en específico por lo que la SUTEL puede disponer de una solución de seguridad que brinde el MFA en diferentes condiciones (Físico, token OTP, etc). 4. Ordenar a la Unidad de Tecnologías de la Información que permita y habilite la utilización del doble factor de autenticación mediante dispositivos tipo token físico, sea que estos sean adquiridos por parte de la institución, o bien, mediante el aporte voluntario de los funcionarios, siempre y cuando se cumpla con los estándares de compatibilidad que la herramienta exige según el principio de neutralidad tecnológica (…)" (ver prueba).
15) En oficio suscrito el **11 de agosto de 2025** por el proveedor Tecnova Soluciones S.A. y remitido a la SUTEL, se consignó lo siguiente:
"(…) En respuesta la consulta sobre la Privacidad del Usuario mencionada en el Anexo 1 del documento RECURSO DE RECONSIDERACIÓN AL ACUERDO N°005-042-2025 DEL 31 DE JULIO DEL 2025, detallamos los siguientes puntos: 1. La Política de Privacidad de Datos de la Aplicación WatchGuard Authpoint se encuentra publicada en el siguiente sitio oficial de WatchGuard Technologies: hLps://www.watchguard.com/es/wgrd-trust-center/privacy-guide/authpoint La consulta de la Política de Privacidad siempre es un recurso obligatorio a la hora de presentar cualquier recurso que tenga que ver con el manejo de datos privados del usuario. 2. Watchguard Technologies cumple la política GDPR de la Unión Europea para todos sus productos, puede encontrar el enunciado en el siguiente sitio web: hLps://www.watchguard.com/es/wgrd-trust-center/gdpr-statement A su vez también publica un Addendum sobre el Procesamiento de Datos de Clientes: hLps://www.watchguard.com/es/wgrd-trust-center/watchguard-technologies-inccustomer-data-processing-addendum 3. La imagen 3 del Anexo muestra un método equivocado para obtener los permisos de acceso de la aplicación WatchGuard Authpoint o cualquier otra aplicación: (…) La forma correcta es acceder a esa misma pantalla y seleccionar los tres puntos ubicados en la esquina superior derecha y seleccionar "Todos los permisos". Esa opción muestra la lista completa de permisos a las que tienen acceso las aplicaciones: (…) Por ejemplo, esta es la lista de permisos totales de la aplicación MicrosoZ Excel en el mismo smarphone, donde se evidencia el acceso a recursos como "have full network access" sin que esto signifique un riesgo de seguridad para el usuario: (…) 4. En cuanto al análisis del APK de Watchguard Authpoint, se parte de una premisa incorrecta: que la simple presencia de términos técnicos en el código de una aplicación equivale a una acción maliciosa. Este enfoque carece de rigor técnico y conduce a conclusiones erróneas y alarmistas que no se corresponden con la realidad operativa de la aplicación. Muy específicamente detallamos los siguientes puntos remitiendo directamente a la Guía de Privacidad oficial de WatchGuard: a. Sobre la Geolocalización y el supuesto "rastreo": i. El análisis sugiere que la aplicación funciona como un "rastreador". Esto es categóricamente falso. La propia política de WatchGuard es explícita: la recopilación de geolocalización precisa (GPS) es opcional y requiere el consentimiento explícito del usuario. Si como usuario no se autoriza este permiso, la función simplemente no se activa. Su único fin, en caso de que una empresa decida usarla, es añadir capas de seguridad adicionales, como permitir autenticaciones solo desde una ubicación específica (por ejemplo permitir las autenticaciones solo desde Costa Rica). b. Sobre la supuesta Captura de Datos Biométricos (Huella/Rostro): i. Según lo explica la guía de privacidad lo explica sin ninguna ambigüedad en la sección "Acceso a identificación biométrica": "No obtenemos acceso a los datos biométricos en sí ni los procesamos." ii. La aplicación utiliza la interfaz segura del sistema operativo del smartphone (Android o iOS). Cuando un usuario pone su huella, el sistema operativo es el que la verifica y únicamente le envía a la app una respuesta de "sí" o "no". La huella dactilar del usuario o sus datos faciales nunca salen de su dispositivo ni son visibles para WatchGuard o para el administrador de la aplicación WatchGuard Authpoint. c. Sobre los Permisos de Cámara y Red: como indica la documentación, los permisos tienen fines justificados y limitados: i. Cámara: Se usa únicamente para que el usuario escanee el código QR al momento de registrar su dispositivo. No hay otra funcionalidad asociada. ii. Red/IP: Es indispensable. La aplicación necesita conectarse a internet para validar en tiempo real que eres tú quien intenta acceder a un servicio protegido. La IP se utiliza, como se ve en la tabla de "Fines del procesamiento", para mejorar la seguridad y detectar intentos de acceso no autorizados. iii. Términos como ip, address, Location o HLpURLConnection son extremadamente comunes en cualquier aplicación que se conecte a internet o utilice servicios de Google. Están presentes en librerías estándar de Android y Google Play Services. Encontrar 84,656 coincidencias de "Red/IP" no significa que la aplicación tenga 84,656 funciones para espiar la IP; significa que el código utiliza librerías de red estándar. Reiteramos que WatchGuard AuthPoint es una herramienta segura, confiable y transparente, diseñada exclusivamente para proteger los accesos corporativos, no para invadir la privacidad de los usuarios, y está certificada como tal (…)" (ver prueba).
16) El **14 de agosto de 2025**, mediante oficio No. 07673-SUTEL-UJ-2025, la Unidad Jurídica de SUTEL emitió criterio jurídico en relación con el recurso de reconsideración presentado por el recurrente y otros funcionarios de esa misma institución (ver prueba).
17) El **19 de agosto de 2025**, el recurrente formuló el presente amparo (ver escrito de interposición).
18) El anterior criterio emitido por la Unidad Jurídica fue acogido por el Consejo de la SUTEL mediante resolución No. RCS-188-2025 adoptada, a su vez, en acuerdo No. 007-046- 2025 de **21 de agosto de 2025**. A través de esta resolución se resolvió el citado recurso de reconsideración, conforme los siguientes términos: *"(…) 1. DECLARAR SIN LUGAR, el recurso de reconsideración interpuesto por los funcionarios de la Dirección General de Calidad en contra del acuerdo 005-042- 2025 del 01 de agosto del 2025. 2. RECHAZAR la medida cautelar solicitada en contra del 005-042-2025 del 01 de agosto del 2025 (…)".* En cuanto al alegato relacionado con la presunta violación a la privacidad y a la protección de datos personales, en esta resolución se indicó expresamente lo siguiente:

"(…) Considerando lo antes dispuesto, se debe aclarar que la medida de seguridad de doble fator de autenticación no es un gestor de información personal ni tiene como uso técnico el análisis de información contenida en los dispositivos que lo instalen, por lo que resulte importante citar la siguiente opinión remitida la UTI: ---------- "Las herramientas de autenticación de doble factor (2FA) son esenciales para fortalecer la seguridad de los sistemas y proteger a la institución contra accesos no autorizados. A diferencia de las contraseñas tradicionales, que pueden ser robadas o descifradas, el 2FA añade una capa adicional de seguridad, exigiendo un segundo factor de verificación, como un código de una aplicación o un mensaje push, antes de conceder acceso. ---------- Los ciberdelincuentes emplean diversas técnicas para robar credenciales, entre ellas: ---------- Ataques de fuerza bruta: Intentos automatizados para descifrar contraseñas mediante combinaciones masivas.---------- Phishing: Engaños a los usuarios para que revelen credenciales a través de correos electrónicos, mensajes o sitios web falsos. ---------- Keylogging: Malware que registra las pulsaciones del teclado para capturar contraseñas y otros datos sensibles. ---------- Ataques de intermediario (Man-in-the-Middle): Interceptación del tráfico entre el usuario y el servidor para robar credenciales. ---------- Credential stuffing: Uso de combinaciones de usuario y contraseña filtradas en otras plataformas para intentar acceder a nuevos servicios. ---------- Para mitigar estos riesgos, se ha implementado la aplicación WatchGuard, que establece las siguientes condiciones en dispositivos móviles: ---------- (…) Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico ---------- El contenido generado por IA puede ser incorrecto. ---------- Permiso para envió de notificaciones push para conexiones con computadoras, VPN u Office 365. ---------- Acceso a la cámara solo para la activación, mediante lectura del código QR. (No pide grabación y/o fotografías del rostro del funcionario) Este permiso lo requieren la mayoría de las aplicaciones en el mercado, solo para citar las más relevantes a nivel institucional: Microsoft Authenticator y a nivel personal, Google Authenticator, Whatsapp y redes sociales en general requieren este tipo de permisos. Además este permiso se puede quitar luego de la instalación de la herramienta si así lo desea el usuario, debido a que es requerido únicamente para la lectura del código QR que asocia la cuenta al dispositivo. - La aplicación no contempla permisos de acceso a archivos, fotos, ni otros datos personales disponibles, en los dispositivos en los cuales se va a instalar. Además el funcionamiento descrito en la ficha técnica de la solución adquirida no incluye el acceso a datos personales, sensibles para su funcionamiento. --- Lo anterior extraído de la página web: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/authpoint/mobile-app_see-device-info.html A pesar de estas medidas, la ciberseguridad es un campo dinámico en constante evolución. Si bien ninguna solución garantiza protección absoluta, la implementación de herramientas como el doble o múltiple factor de autenticación reduce significativamente los riesgos y fortalece la seguridad de la información institucional (…)". (Correo electrónico del 20 de febrero del año en curso). ---------- De conformidad con lo antes expuesto, es procedente indicar que el doble factor de autenticación no tiene como fin: gestionar, regular o utilizar información sensible de quienes lo instalen, por lo que carece de relación con aquellas garantías previstas en el artículo 24 de la C.P., sin embargo, se destaca que la instalación de la herramienta establece las condiciones de uso, mediante las cuales los eventuales usuarios se ven debidamente informados de los accesos de la aplicación." ---------- De conformidad con lo anterior, el argumento se debe rechazar. ---------- (…)" (ver prueba).

19) El **28 de agosto de 2025**, la parte recurrida fue notificada de la interposición de este amparo (ver acta de notificación).

20) El **28 de agosto de 2025**, el Jefe de Tecnología de Información de la SUTEL le remitió varias manifestaciones al Director Nacional de Ciberseguridad. Entre otros aspectos, en esta ocasión, se indicó: *"(…) La Unidad de TI nunca ha afirmado que los tokens físicos no sean compatibles con la plataforma WatchGuard AuthPoint. No obstante, como ha señalado la Unidad Jurídica de SUTEL en varios oficios, la contratación 2023LE-000002-001490001 fue un proceso de licitación pública que siguió el debido procedimiento en el sistema de compras gubernamentales (SICOP) y no fue impugnado por ningún funcionario durante el proceso de cartel. La plataforma sí tiene la capacidad técnica para integrarse con tokens físicos; sin embargo, la Unidad de TI determinó, con base en criterios técnicos y de costo beneficio, que el método de MFA se implementaría mediante la aplicación móvil (…)"* (ver prueba).

21) El **31 de agosto de 2025**, ante una consulta realizada por SUTEL, el Director Nacional de Ciberseguridad del MICITT, señaló lo siguiente:

"(…) Agradezco el contexto remitido respecto al uso de autenticación multifactor (MFA) y, en particular, la integración de WatchGuard AuthPoint adquirida mediante la contratación 2023LE-000002-001490001. Como criterio técnico y en coherencia con la Directriz MICITT-DGDCFD-DRII-AT-082-2024, reitero que cada institución, por medio de su departamento de TI, es la responsable de valorar el riesgo, definir e implementar las soluciones de seguridad que correspondan a su realidad operativa, siempre que cumplan los controles mínimos establecidos. Ello obedece a que los recursos presupuestarios, el personal y los factores técnicos son conocidos en detalle por la jefatura de TI, quien es la autoridad técnica y el máximo responsable de la gestión, configuración y correcta implementación de las plataformas y controles de seguridad Cuando existe una compra institucional vigente como la señalada, su despliegue demuestra el debido cuidado y la debida diligencia (due care/due diligence) para proteger el acceso a servicios críticos (PC, VPN, correo, entre otros) mediante el control 2FA definido por el departamento responsable. En ese escenario corresponde hacer uso eficiente de los recursos ya invertidos y operar el control conforme al marco contractual y a las mejores prácticas, incluidos los procesos de soporte, mantenimiento y niveles de servicio provistos por el adjudicatario. La directriz no prescribe marcas ni impone un único método de MFA; exige controles efectivos. Si el análisis técnico y de costo-beneficio de la Unidad de TI determinó que la verificación por notificación push de AuthPoint es la opción adecuada para integrar con el perímetro y la VPN institucional, y dicha configuración cumple los mínimos exigidos (registro seguro del segundo factor, protección contra suplantación, trazabilidad, revocación oportuna y soporte), el enfoque es válido. Respecto de los tokens físicos, no están excluidos per se, siempre que su uso se gestione bajo administración institucional y por medio de procesos de contratación que aseguren soporte, ciclo de vida, inventario y cumplimiento. En cambio, incorporar tokens adquiridos a título personal, fuera de la contratación vigente, no es recomendable por los riesgos y vacíos de control que introduce. Entre los riesgos adicionales que deben considerarse se encuentran la ausencia de SLA y garantías del proveedor y del ciclo de vida del segundo

factor (altas, bajas, revocación inmediata ante cambios o pérdidas); afectaciones a la continuidad operativa si no existen métodos de respaldo (TOTP/FIDO2), cuentas de emergencia controladas y pruebas periódicas; riesgos en la cadena de suministro al adquirir dispositivos por canales no verificados; y compromisos de interoperabilidad y experiencia de usuario que deben balancearse sin sacrificar controles. Por lo cual, se recomienda que todo control debe ser valorado de previo por el departamento responsable en este caso el departamento de informática, responsable de brindar soporte a los elementos tecnológicos de la institución. En términos operativos, resulta conveniente normar en un documento institucional los métodos MFA permitidos (Política de Control de acceso), ya que esto puede abrir puertas para que el personal no informático, tome decisiones cuál método desea y no el que la institución defina. Asimismo, corresponde recordar que el departamento de informática es el administrador del contrato y el responsable del soporte del bien adquirido en la 2023LE-000002-001490001, debiendo velar porque el control funcione conforme a lo contratado o, en su caso, escalar y exigir el soporte que está previsto en dicha contratación. En contraste, una adquisición que no forme parte del bien institucional y por la cual el departamento de TI no sea responsable, puede constituir un riesgo operativo, legal y de sostenibilidad del control por carecer de cobertura formal de soporte y gobierno. A la luz de la circular MIDEPLA-DM-CIRC-004-2025-MICITT-DM-2025, mis respuestas no excluyen métodos específicos ya que el MICITT es agnósticos a las soluciones de seguridad y respetuoso de los procesos de cada institución que conocen su contexto y recursos. Por lo cual el MICITT requiere que se garantice la aplicación del control de seguridad que minimicen los riesgos de seguridad en estos vectores; enfatiza la responsabilidad del departamento de TI de seleccionar e instrumentar el mecanismo de MFA que resulte idóneo para su contexto, cumpliendo los mínimos exigidos por la directriz y aprovechando los recursos institucionales en este caso la contratación institucional vigente. Por estas razones, la incorporación de tokens personales fuera del marco contractual no se recomienda. Respetando el marco de competencias y lo señalado, se recomienda que la Unidad de TI, como autoridad técnica, valore el riesgo y defina el mecanismo de MFA adecuado, asegurando el cumplimiento de la directriz del MICITT y su gestión conforme a los instrumentos legales pertinentes (…)" (ver informe y prueba).

22) Para el día de rendido el informe por la parte recurrida, sea, el **2 de septiembre de 2025**, el accionante era el único funcionario de la SUTEL que se oponía a instalar el doble factor de autenticación en su dispositivo móvil como requisito para efectuar el teletrabajo (ver informe).

III.- HECHOS NO PROBADOS. De relevancia para dirimir el presente recurso de amparo, se tienen por acreditados los siguientes:

1) Que un determinado día (antes de formulado este amparo) el tutelado haya presentado alguna gestión ante la parte recurrida tocante a la instalación del dispositivo en cuestión y que esta no se haya atendido o respondido (los autos).

2) Que con la instalación de la aplicación alegada en los celulares de los funcionarios de la SUTEL, se pueda tener acceso concomitante a la información personal de estos últimos (los autos).

IV.- CASO CONCRETO. El tutelado, quien labora para la SUTEL como Jefe de la Dirección General de Calidad, acude a esta Sala y señala que los jerarcas de dicha entidad obligaron a los funcionarios a utilizar o instalar en sus dispositivos móviles personales la aplicación AuthPoint de WatchGuard como mecanismo de doble factor de autenticación (en lugar de hacer uso de otros medios también disponibles), como medio para realizar teletrabajo. Indica que, por ejemplo, podría permitirse el uso de tokens físicos, que cumplen con el mismo propósito y fueron autorizados en su momento por la SUTEL.

Alega que se desconoce el alcance de dicha aplicación y la interacción que podría tener con otras aplicaciones y datos personales del funcionario que se encuentran en su teléfono, por lo que estima vulnerado lo dispuesto en el artículo 24 de la Constitución Política (y sus derechos a la intimidad, a la inviolabilidad de documentos y al secreto de las comunicaciones, etc.). Sostiene que, para el tratamiento de datos personales, se requiere de la emisión del respectivo consentimiento e, incluso, una orden judicial o habilitación de legislación especial.

Acusa que el Consejo de SUTEL no ha emitido un pronunciamiento expreso sobre los motivos por los cuales no se considera su propuesta (en cuanto a utilizar otro mecanismo de autenticación).

Finalmente, sostiene que la parte recurrida expuso su nombre, como parte del grupo de funcionarios que se opusieron a dicha medida, señalándose, además, las consecuencias a las que se expone si no acata lo ordenado; actuación que, en su criterio, se traduce en una sanción moral. Alega que se trató de una medida unilateral, coercitiva, sorpresiva e innecesaria y no se les brindó posibilidad de ejercer el derecho a la defensa.

Por todo lo anterior, solicita que se declare con lugar el recurso y se le ordene al Consejo de la SUTEL "*dejar sin efecto la disposición relacionada con la instalación de una aplicación únicamente en los teléfonos celulares personales de sus funcionarios por ser contraria a las disposiciones constitucionales señaladas".*

Revisados los argumentos expuestos por el recurrente, el informe rendido bajo la solemnidad de juramento por el Presidente del Consejo y representante judicial y extrajudicial de la Superintendencia de Telecomunicaciones, así como todas las pruebas aportadas, este Tribunal Constitucional no considera que exista mérito para acoger este proceso de amparo. Lo anterior, por lo motivos que se explicarán a continuación.

A. En cuanto a la decisión de utilizar sistema de doble factor de autenticación mediante el uso de una aplicación instalada en los teléfonos móviles personales de los funcionarios de la SUTEL que desean realizar teletrabajo (y no mediante el uso de tokens físicos). Tema de mera legalidad. Según se logra desprender con meridiana claridad del estudio del informe rendido por la parte recurrida y del elenco de hechos probados, el Consejo de la SUTEL acordó en julio de este año 2025 que aquellos funcionarios que deseen acogerse al teletrabajo debían instalar en sus teléfonos móviles personales una aplicación de doble factor de verificación como mecanismo de seguridad. También se demostró que, aun cuando se podría utilizar tokens físicos para tales efectos, la autoridad recurrida se decantó finalmente por la instalación de la referida aplicación en los teléfonos celulares de los funcionarios. Según se consignó, la Unidad de Tecnología de Información de la SUTEL determinó, con base en criterios técnicos y de costo-beneficio, que el método de autenticación multifactor se implementaría mediante una aplicación móvil. En consuno con lo anterior, el Presidente del Consejo y representante judicial y extrajudicial de la Superintendencia de Telecomunicaciones sostuvo en el informe rendido que *"(…) la decisión de no considerar tokens físicos responde a un análisis técnico y de adopción previa, Asimismo, se consideró que el uso de esa herramienta en los dispositivos*

móviles es la mejor opción por temas de eficiencia, costo y versatilidad para todas las partes (…)".
Analizado lo anterior, esta Sala Constitucional considera que no le corresponde –por tratarse de un tema de pura y mera legalidad–, realizar un análisis por el fondo, concretamente, respecto a los criterios técnicos que respaldan el uso de mecanismos de autenticación multifactor mediante la instalación propiamente de una aplicación electrónica o bien, mediante el uso de token físico y determinar finalmente cuál de estos es el más apropiado o adecuado a efecto de lograr los fines señalados por la SUTEL. Tampoco, le corresponde a esta jurisdicción cuestionar el criterio de oportunidad y conveniencia de la administración recurrida para utilizar el factor de doble autenticación mediante la instalación de una aplicación en los celulares y no permitir el uso de tokens físicos. Mucho menos, desde esa perspectiva, podría este Tribunal finalmente acoger la pretensión del recurrente y ordenarle a la SUTEL dejar sin efecto la disposición en cuestión y permitirle, en su caso y excepcionalmente, hacer uso del token físico.
Claramente estamos frente a una decisión institucional sustentada en múltiples criterios e informes técnicos (tal y como se comprobó en el apartado de hechos probados de esta sentencia), respecto a la cual el tutelado se encuentra disconforme y respecto a la cual, si a bien lo tiene, puede plantear los alegatos que estime pertinentes ante las vías ordinarias de legalidad administrativas y jurisdiccionales creadas especialmente al efecto.

B. Fundamentación de la decisión reclamada. Cabe destacar que la decisión de la SUTEL respecto a la cual se encuentra disconforme el recurrente (obligación de instalar en su celular personal una aplicación de doble factor de autenticación llamada AuthPoint de WatchGuard), no se encuentra carente de sustento ni se podría tildar *prima facie* de arbitraria. Por el contrario, se ha demostrado que dicha medida se ha gestionado e implementado por motivos de seguridad y en aras de prevenir ataques cibernéticos y garantizar el resguardo, protección e integridad de los datos y equipos propiedad de la institución. En cuanto a este aspecto, en el oficio No. 01480-SUTEL-UJ-2025 de 20 febrero de 2025 suscrito por parte de la Unidad Jurídica de la SUTEL se consignó lo siguiente
*"(…) **el objetivo es fortalecer la seguridad de la información y proteger los datos sensibles y equipos de la SUTEL**. Asimismo, el fin de la herramienta de seguridad indicada, se deriva de las diversas directrices emitidas por el MICITT y el criterio técnico de la Unidad de Tecnologías de Información de la SUTEL (…)*
el uso de la doble autenticación a través de dispositivos móviles se presenta como una solución adecuada para mitigar el riesgo en la vulneración de equipos, sistemas y dato de la entidad (…)
Las herramientas solicitadas son instrumentos básicos para la protección de la información institucional y el resguardo de la operación técnica de la SUTEL (…)
***La herramienta de autenticación multifactor (MFA) es fundamental para reforzar la seguridad en el acceso a sistemas y datos sensibles.** Al requerir múltiples formas de verificación más allá de las contraseñas, como códigos temporales o notificaciones push, el MFA **reduce el riesgo de violaciones de seguridad, protege la información confidencial y cumple con regulaciones del Código Nacional de Tecnologías Digitales Capítulo 2 Identificación y Autenticación Ciudadana. Además, en un entorno laboral remoto, garantiza un acceso seguro desde ubicaciones externas**. Esta capa adicional de seguridad no solo fortalece la protección de datos, sino que también mejora la experiencia del usuario al proporcionar un acceso seguro sin comprometer la usabilidad una vez que se integra adecuadamente (…)"* (El destacado no forma parte del original).

Por su parte, el Presidente del Consejo y representante de la Superintendencia de Telecomunicaciones aseveró en su informe lo siguiente:
*"(…) Cabe recalcar que el **no implementar el método de doble factor de autenticación (2FA) representa un riesgo crítico para la seguridad de la información en cualquier organización**. Confiar únicamente en contraseñas expone a los sistemas institucionales a ataques comunes como el phishing, el robo de credenciales, o el uso de contraseñas reutilizadas, facilitando accesos no autorizados a información sensible, servicios críticos o recursos internos. Este tipo de brechas puede derivar en pérdida de información confidencial, continuidad operativa, daño reputacional e incluso sanciones regulatorias, especialmente en el sector de gobierno como lo es SUTEL. **La implementación de 2FA mitiga significativamente estos riesgos al requerir una segunda forma de verificación mediante una aplicación autenticadora**. Esto bloquea vectores de ataque como el robo de contraseñas, los intentos de fuerza bruta, y los accesos indebidos incluso si las credenciales han sido comprometidas. **Adoptar 2FA es una de las medidas más efectivas y de bajo costo para fortalecer la postura de ciberseguridad y proteger tanto a los usuarios como a la organización** (…)*
*la Unidad de Tecnologías de Información (…) emitió el criterio técnico que justifica la implementación de la herramienta denominada WatchGuard Authpoint en los dispositivos móviles personales de los funcionarios, como requisito para realizar el doble factor de autenticación y permitir a los funcionarios laborar en la modalidad de teletrabajo. **De dicho criterio técnico, se extrae que el requerimiento en análisis tiene como objetivo principal velar por el interés público, al fortalecer la seguridad de la información y proteger los datos sensibles y equipos de la Sutel ante las continuas violaciones y hackeos de información que se han dado a nivel nacional**. Asimismo, la implementación de la herramienta de seguridad indicada **se deriva de las diversas directrices y lineamientos emitidos por el MICITT y el MIDEPLAN, que, provienen de marcos regulatorios que rigen a todas las instituciones públicas** (…)"* El destacado no forma parte del original).

Aunado a ello, no puede perderse de vista que la obligación impuesta a los funcionarios recurridos tiene sustento, a su vez, en la normativa que regula el teletrabajo. En ese particular, en el citado oficio No. 01480-SUTEL-UJ-2025 de 20 febrero de 2025, la Unidad Jurídica de la SUTEL explicó lo siguiente:
"(…) La Ley para regular el teletrabajo, Ley N° 9738, aplica para la Sutel, según lo que establece el artículo 2. Por lo tanto, es aplicable lo dispuesto en el artículo 9 inciso a) que establece lo siguiente: "Artículo 9- Obligaciones de las personas teletrabajadoras. Sin perjuicio de las demás obligaciones que acuerden las partes en el contrato o adenda de teletrabajo, serán obligaciones para las personas teletrabajadoras las siguientes: a) Cumplir con los criterios de medición, evaluación y control determinados en el contrato o adenda, así como sujetarse a las políticas y los códigos de la empresa, respecto a temas de

relaciones laborales, comportamiento, confidencialidad, manejo de la información y demás disposiciones aplicables."
El Reglamento para regular el teletrabajo, decreto Nº 42083-MP-MTSS-MIDEPLAN-MICITT, en el artículo 6 establece los deberes de las personas teletrabajadoras y indica que las personas teletrabajadoras deben cumplir lo siguiente: b) Las demás obligaciones contenidas en el contrato o adenda de teletrabajo y la legislación costarricense.
De acuerdo con esa ley y reglamento, es una obligación de las personas que teletrabajan cumplir con las políticas que emita la institución, por lo que, esas normas se deben complementar con las regulaciones emitidas por la Sutel El Reglamento de Teletrabajo en la Autoridad Reguladora de los Servicios Públicos y su órgano desconcentrado (en adelante Reglamento de Teletrabajo), el cual resulta aplicable a SUTEL, dispone en lo relevante lo siguiente: "Artículo 5.- Dependencias de apoyo de la CIT y sus funciones. Son dependencias de apoyo las que a continuación se indican y tendrán las funciones siguientes: (…) b) Tecnologías de Información, se encargará de: (…) 4) Definir, actualizar y comunicar oportunamente las condiciones mínimas de tecnologías de información y comunicación con las que debe contar la persona teletrabajadora en el centro o lugar de teletrabajo, incluidas las medidas de seguridad informática".
De conformidad con el reglamento antes citado, el establecimiento de condiciones mínimas en tecnologías de información que la Unidad de Tecnología de Información (en adelante UTI) defina mediante criterio técnico para personas que, voluntariamente, desean acceder a la modalidad de teletrabajo, se encuentra contemplado en la normativa específica que aplica a la SUTEL, por lo que resulta posible. Además, se destaca que el Reglamento de Teletrabajo contempla las obligaciones del funcionario en teletrabajo y, en lo que interesa dispone lo siguiente: "Artículo 2. Alcance. El presente reglamento es de acatamiento obligatorio para todas las personas funcionarias de la Autoridad Reguladora de los Servicios Públicos y su órgano desconcentrado que voluntariamente soliciten la aprobación del teletrabajo como una modalidad de trabajo a distancia mediante el uso de medios y tecnología de la información y comunicación (…) Artículo 6. - Condiciones generales del teletrabajo. Las condiciones generales del teletrabajo son las siguientes: (…) e) Requiere el uso y cumplimiento de las condiciones mínimas vigentes establecidas por tecnologías de información y salud ocupacional en el lugar o centro de teletrabajo para acceder a la modalidad de teletrabajo. (…) ***Artículo 10.- Requisitos de la persona teletrabajadora. La persona funcionaria que solicite el teletrabajo deberá cumplir con cada uno de los requisitos siguientes: (…) d) Cumplir con los lineamientos específicos emitidos por la CIT y las dependencias de apoyo en materia de tecnologías de la información y comunicación y de salud ocupacional. (…)***
Artículo 12.- Obligaciones de la persona teletrabajadora (…) b) Tramitar una adenda al contrato de teletrabajo en caso de que varíe alguna de las condiciones que justificaron su ingreso a la modalidad de teletrabajo (lugar o centro de teletrabajo estipulado, cambio de puesto, actividades o condiciones mínimas de tecnologías de información y salud ocupacional requeridas, así como el cambio permanente en los días de teletrabajo estipulados). El teletrabajo se continuará realizando hasta que se apruebe la adenda al contrato (…)".
***Lo anterior implica que, una vez que se defina algún requerimiento mínimo en tecnologías de información como requisito para acceder a la modalidad de teletrabajo de parte de UTI, los colaboradores que deseen estar en dicha modalidad deben cumplir con ese requisito** (…)"* (El destacado no forma parte del original).

C. Sobre la presunta violación a lo dispuesto en el ordinal 24 constitucional. Como punto medular de este amparo, el recurrente manifiesta que la instalación de la aplicación en cuestión en su teléfono celular (aplicación AuthPoint de WatchGuard como mecanismo de doble factor de autenticación), violenta sus derechos a la intimidad y a la autodeterminación informativa. Particularmente, sostiene que desconoce el alcance de sus funciones y la interacción que podría tener con otras aplicaciones y datos personales del funcionario que se encuentran en su móvil. Alega que se podría permitir el acceso a datos e información vinculada a los celulares, tales como geolocalización, desplazamientos e, incluso, en algunos casos, datos relacionados con la salud y la condición física del titular del aparato.
No obstante, esta Sala no estima de recibido este agravio. Primero, por cuanto el tutelado no hizo referencia a un hecho en concreto (con sustento probatorio), sino a un hecho futuro e incierto, sea, sobre la eventual posibilidad de que, al instalársele la aplicación bajo estudio, se acceda a su información personal contenida en el celular. Como bien lo informó la parte recurrida, se trata de meras suposiciones o conjeturas que no fueron respaldadas, además, con ningún fundamento o sustento técnico y probatorio. Segundo, dado que, contrario a lo que sostiene el recurrente, el Presidente del Consejo de la Superintendencia de Telecomunicaciones informó bajo juramento (con sustento en varios oficios y pruebas adjuntas), que, a través de dicha aplicación, no se acceden a los datos que reclama el tutelado.
En ese particular, es importante señalar que en el oficio No. 09751-SUTEL-DGO-2024 de fecha 4 de noviembre de 2024 suscrito por la Jefatura de la Unidad Jurídica y la Jefatura de la Unidad de Tecnologías de Información de SUTEL, se consignó, al respecto, lo siguiente:
"(…) 4. DE LA HERRAMIENTA CONTRATADA MEDIANTE EL PROCEDIMIENTO DE CONTRATACIÓN NO. 2023LE-000002-00149000 B. DE LAS CARACTERÍSTICAS DE LA HERRAMIENTA Es importante recalcar que, la herramienta utiliza como método de autenticación, el dispositivo móvil, celular o smartphone, mediante la aplicación Authpoint y que, se utiliza, exclusivamente, para que el usuario valide su identidad al acceder a los sistemas. Mediante una sola aplicación, se puede validar el acceso a la computadora, a las herramientas colaborativas de Microsoft, como Teams y Outlook y, por último, la VPN.
Adicionalmente, se debe aclarar que ***la herramienta no tiene las siguientes funcionalidades: determinar la ubicación del dispositivo, realizar una intrusión en el sistema operativo del dispositivo móvil donde se instala u obtener información privada del funcionario, es únicamente, un método para verificar la identidad del funcionario*** *(…)"* (El destacado no forma parte del original).

Por su parte, en el oficio No. 01480-SUTEL-UJ-2025 de 20 febrero de 2025, la Unidad Jurídica de la SUTEL consignó:
"(…) se debe aclarar que la ***medida de seguridad de doble factor de autenticación no es un gestor de información personal ni tiene como uso técnico el análisis de información contenida en los dispositivos que lo instalen****, por lo que resulte importante citar la siguiente opinión remitida la UTI: "Las herramientas de autenticación de doble factor (2FA) son esenciales para fortalecer la*

seguridad de los sistemas y proteger a la institución contra accesos no autorizados. A diferencia de las contraseñas tradicionales, que pueden ser robadas o descifradas, el 2FA añade una capa adicional de seguridad, exigiendo un segundo factor de verificación, como un código de una aplicación o un mensaje push, antes de conceder acceso. Los ciberdelincuentes emplean diversas técnicas para robar credenciales, entre ellas: Ataques de fuerza bruta: Intentos automatizados para descifrar contraseñas mediante combinaciones masivas. Phishing: Engaños a los usuarios para que revelen credenciales a través de correos electrónicos, mensajes o sitios web falsos. Keylogging: Malware que registra las pulsaciones del teclado para capturar contraseñas y otros datos sensibles. Ataques de intermediario (Man-in-the-Middle): Interceptación del tráfico entre el usuario y el servidor para robar credenciales. Credential stuffing: Uso de combinaciones de usuario y contraseña filtradas en otras plataformas para intentar acceder a nuevos servicios. Para mitigar estos riesgos, se ha implementado la aplicación WatchGuard, que establece las siguientes condiciones en dispositivos móviles: (…) Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico El contenido generado por IA puede ser incorrecto. Permiso para envió de notificaciones push para conexiones con computadoras, VPN u Office 365. Acceso a la cámara solo para la activación, mediante lectura del código QR. (No pide grabación y/o fotografías del rostro del funcionario) Este permiso lo requieren la mayoría de las aplicaciones en el mercado, solo para citar las más relevantes a nivel institucional: Microsoft Authenticator y a nivel personal, Google Authenticator, Whatsapp y redes sociales en general requieren este tipo de permisos. Además este permiso se puede quitar luego de la instalación de la herramienta si así lo desea el usuario, debido a que es requerido únicamente para la lectura del código QR que asocia la cuenta al dispositivo. ***La aplicación no contempla permisos de acceso a archivos, fotos, ni otros datos personales disponibles, en los dispositivos en los cuales se va a instalar. Además el funcionamiento descrito en la ficha técnica de la solución adquirida no incluye el acceso a datos personales, sensibles para su funcionamiento.*** *(…) A pesar de estas medidas, la ciberseguridad es un campo dinámico en constante evolución. Si bien ninguna solución garantiza protección absoluta, la implementación de herramientas como el doble o múltiple factor de autenticación reduce significativamente los riesgos y fortalece la seguridad de la información institucional (…)". (Correo electrónico del 20 de febrero del año en curso). De conformidad con lo antes expuesto, es procedente indicar que* ***el doble factor de autenticación no tiene como fin: gestionar, regular o utilizar información sensible de quienes lo instalen, por lo que carece de relación con aquellas garantías previstas en el artículo 24 de la C.P****. Además, se destaca que la instalación de la herramienta establece las condiciones de uso, mediante las cuales los eventuales usuarios se ven debidamente informados de los accesos de la aplicación (…)"* (El destacado no forma parte del original).

Igualmente, la autoridad recurrida aportó a este proceso un oficio de fecha 11 de agosto de 2025 suscrito por el proveedor Tecnova Soluciones S.A. en el cual, sobre el tema bajo estudio, se indicó lo siguiente:
"(…) En respuesta la consulta sobre la Privacidad del Usuario mencionada en el Anexo 1 del documento RECURSO DE RECONSIDERACIÓN AL ACUERDO N°005-042-2025 DEL 31 DE JULIO DEL 2025, detallamos los siguientes puntos: 1. La Política de Privacidad de Datos de la Aplicación WatchGuard Authpoint se encuentra publicada en el siguiente sitio oficial de WatchGuard Technologies: hLps://www.watchguard.com/es/wgrd-trust-center/privacy-guide/authpoint La consulta de la Política de Privacidad siempre es un recurso obligatorio a la hora de presentar cualquier recurso que tenga que ver con el manejo de datos privados del usuario. 2. Watchguard Technologies cumple la política GDPR de la Unión Europea para todos sus productos, puede encontrar el enunciado en el siguiente sitio web: hLps://www.watchguard.com/es/wgrd-trust-center/gdpr-statement A su vez también publica un Addendum sobre el Procesamiento de Datos de Clientes: hLps://www.watchguard.com/es/wgrd-trust-center/watchguard-technologies-inccustomer-data-processing-addendum 3. La imagen 3 del Anexo muestra un método equivocado para obtener los permisos de acceso de la aplicación WatchGuard Authpoint o cualquier otra aplicación: (…) La forma correcta es acceder a esa misma pantalla y seleccionar los tres puntos ubicados en la esquina superior derecha y seleccionar "Todos los permisos". Esa opción muestra la lista completa de permisos a las que tienen acceso las aplicaciones: (…) Por ejemplo, esta es la lista de permisos totales de la aplicación MicrosoZ Excel en el mismo smarphone, donde se evidencia el acceso a recursos como "have full network access" sin que esto signifique un riesgo de seguridad para el usuario: (…) 4. En cuanto al análisis del APK de Watchguard Authpoint, se parte de una premisa incorrecta: que la simple presencia de términos técnicos en el código de una aplicación equivale a una acción maliciosa. Este enfoque carece de rigor técnico y conduce a conclusiones erróneas y alarmistas que no se corresponden con la realidad operativa de la aplicación.
Muy específicamente detallamos los siguientes puntos remitiendo directamente a la Guía de Privacidad oficial de WatchGuard:
a. Sobre la Geolocalización y el supuesto "rastreo": *i. El análisis sugiere que la aplicación funciona como un "rastreador". Esto es categóricamente falso. La propia política de WatchGuard es explícita: la recopilación de geolocalización precisa (GPS) es opcional y requiere el consentimiento explícito del usuario. Si como usuario no se autoriza este permiso, la función simplemente no se activa. Su único fin, en caso de que una empresa decida usarla, es añadir capas de seguridad adicionales, como permitir autenticaciones solo desde una ubicación específica (por ejemplo permitir las autenticaciones solo desde Costa Rica).*
b. Sobre la supuesta Captura de Datos Biométricos (Huella/Rostro): *i. Según lo explica la guía de privacidad lo explica sin ninguna ambigüedad en la sección "Acceso a identificación biométrica": "No obtenemos acceso a los datos biométricos en sí ni los procesamos." ii. La aplicación utiliza la interfaz segura del sistema operativo del smartphone (Android o iOS). Cuando un usuario pone su huella, el sistema operativo es el que la verifica y únicamente le envía a la app una respuesta de "sí" o "no". La huella dactilar del usuario o sus datos faciales nunca salen de su dispositivo ni son visibles para WatchGuard o para el administrador de la aplicación WatchGuard Authpoint.*
c. Sobre los Permisos de Cámara y Red*: como indica la documentación, los permisos tienen fines justificados y limitados: i. Cámara: Se usa únicamente para que el usuario escanee el código QR al momento de registrar su dispositivo. No hay otra funcionalidad asociada. ii. Red/IP: Es indispensable. La aplicación necesita conectarse a internet para validar en tiempo real que eres tú quien intenta acceder a un servicio protegido. La IP se utiliza, como se ve en la tabla de "Fines del procesamiento", para mejorar la seguridad y detectar intentos de acceso no autorizados. iii. Términos como ip, address, Location o HLpURLConnection son extremadamente comunes en cualquier aplicación que se conecte a internet o utilice servicios de Google. Están presentes en librerías estándar de Android y Google Play Services. Encontrar 84,656 coincidencias de "Red/IP" no significa que la aplicación*

tenga 84,656 funciones para espiar la IP; significa que el código utiliza librerías de red estándar.
Reiteramos que WatchGuard AuthPoint es una herramienta segura, confiable y transparente, diseñada exclusivamente para proteger los accesos corporativos, no para invadir la privacidad de los usuarios, y está certificada como tal *(…)"* (El destacado no forma parte del original).

En la resolución No. RCS-188-2025 de 21 de agosto de 2025 (emitida con motivo de una impugnación formulada por el recurrente y otros funcionarios de la SUTEL), el Consejo de la SUTE señaló también lo siguiente en cuanto al alegato relacionado con la presunta violación a la privacidad y a la protección de datos personales:
"(…) ***Considerando lo antes dispuesto, se debe aclarar que la medida de seguridad de doble fator de autenticación no es un gestor de información personal ni tiene como uso técnico el análisis de información contenida en los dispositivos que lo instalen****, por lo que resulte importante citar la siguiente opinión remitida la UTI: ---------- "Las herramientas de autenticación de doble factor (2FA) son esenciales para fortalecer la seguridad de los sistemas y proteger a la institución contra accesos no autorizados. A diferencia de las contraseñas tradicionales, que pueden ser robadas o descifradas, el 2FA añade una capa adicional de seguridad, exigiendo un segundo factor de verificación, como un código de una aplicación o un mensaje push, antes de conceder acceso. ---------- Los ciberdelincuentes emplean diversas técnicas para robar credenciales, entre ellas: ---------- Ataques de fuerza bruta: Intentos automatizados para descifrar contraseñas mediante combinaciones masivas.---------- Phishing: Engaños a los usuarios para que revelen credenciales a través de correos electrónicos, mensajes o sitios web falsos. ---------- Keylogging: Malware que registra las pulsaciones del teclado para capturar contraseñas y otros datos sensibles. ---------- ---------- Ataques de intermediario (Man-in-the-Middle): Interceptación del tráfico entre el usuario y el servidor para robar credenciales. ---------- Credential stuffing: Uso de combinaciones de usuario y contraseña filtradas en otras plataformas para intentar acceder a nuevos servicios. ---------- Para mitigar estos riesgos, se ha implementado la aplicación WatchGuard, que establece las siguientes condiciones en dispositivos móviles: ---------- (…) Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico ---------- El contenido generado por IA puede ser incorrecto. ---------- ---------- Permiso para envió de notificaciones push para conexiones con computadoras, VPN u Office 365. ---------- ----------* ***Acceso a la cámara solo para la activación, mediante lectura del código QR. (No pide grabación y/o fotografías del rostro del funcionario)*** *Este permiso lo requieren la mayoría de las aplicaciones en el mercado, solo para citar las más relevantes a nivel institucional: Microsoft Authenticator y a nivel personal, Google Authenticator, Whatsapp y redes sociales en general requieren este tipo de permisos.* ***Además este permiso se puede quitar luego de la instalación de la herramienta si así lo desea el usuario, debido a que es requerido únicamente para la lectura del código QR que asocia la cuenta al dispositivo. - La aplicación no contempla permisos de acceso a archivos, fotos, ni otros datos personales disponibles, en los dispositivos en los cuales se va a instalar****. Además el funcionamiento descrito en la ficha técnica de la solución adquirida no incluye el acceso a datos personales, sensibles para su funcionamiento. --- Lo anterior extraído de la página web: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/authpoint/mobile-app_see-device-info.html A pesar de estas medidas, la ciberseguridad es un campo dinámico en constante evolución. Si bien ninguna solución garantiza protección absoluta, la implementación de herramientas como el doble o múltiple factor de autenticación reduce significativamente los riesgos y fortalece la seguridad de la información institucional (…)". (Correo electrónico del 20 de febrero del año en curso). ---------- ----------* ***De conformidad con lo antes expuesto, es procedente indicar que el doble factor de autenticación no tiene como fin: gestionar, regular o utilizar información sensible de quienes lo instalen, por lo que carece de relación con aquellas garantías previstas en el artículo 24 de la C.P****., sin embargo, se destaca que la instalación de la herramienta establece las condiciones de uso, mediante las cuales los eventuales usuarios se ven debidamente informados de los accesos de la aplicación (…)"* (El destacado no forma parte del original).

De esta manera, se demuestra también que al recurrente ya le han explicado que la aplicación no accede o manipula información personal y sensible del usuario.
En ese mismo orden de consideraciones, cabe destacar que, de forma contundente, el Presidente del Consejo y representante judicial y extrajudicial de la Superintendencia de Telecomunicaciones, informó bajo la solemnidad de juramento a esta Sala, lo siguiente:
"(…) dicha aplicación puede ver la siguiente información del dispositivo móvil: datos técnicos del dispositivo móvil; permiso para envío de notificaciones push para conexiones con computadoras, VPN u Office 365 y; acceso a la cámara solo para la activación, mediante lectura del código QR (cabe recalcar que no pide grabación y/o fotografías del rostro del funcionario). Este permiso lo requieren la mayoría de las aplicaciones en el mercado, solo para citar las más relevantes a nivel institucional: Microsoft Authenticator y a nivel personal, Google Authenticator, Whatsapp y redes sociales en general requieren este tipo de permisos. ***Además, este permiso se puede quitar luego de la instalación de la herramienta si así lo desea el usuario, debido a que es requerido únicamente para la lectura del código QR que asocia la cuenta al dispositivo. Cabe agregar que la aplicación no contempla permisos de acceso a archivos, fotos, ni otros datos personales disponibles, en los dispositivos en los cuales se va a instalar. Aunado a esto, el funcionamiento descrito en la ficha técnica de la solución adquirida no incluye el acceso a datos personales, sensibles para su funcionamiento****. Lo anterior, la UTI lo extrajo de la página web: https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/authpoint/mobile-app_see-device-info.html y además, este criterio técnico se hizo constar en el oficio emitido por la jefatura de la Unidad de Tecnologías de Información y de la Unidad Jurídica de la Sutel, número 09751-SUTEL-DGO-2024 del 4 de noviembre de 2024 y en el oficio 01480-SUTEL-UJ-2025, emitido el 20 de febrero del 2025 por la Unidad Jurídica (…)*
De conformidad con lo antes expuesto, ***es posible concluir con meridiana claridad que el doble factor de autenticación no gestiona, regula o utiliza información sensible de quienes lo instalen, por lo que no trasgrede las garantías reguladas en el artículo 24 de la Constitución Política****. Además, dicha aplicación establece las condiciones de uso, mediante las cuales los*

eventuales usuarios se ven debidamente informados de los accesos de la aplicación (…)" (El destacado no forma parte del original).

Finalmente, es importante apuntar que, en este caso, resulta aplicable lo dispuesto por este Tribunal, por ejemplo, en el Voto No. 2023-29772 de las 09:30 hrs. de 17 de noviembre de 2023; ocasión en la cual se señaló lo siguiente:
"(…) ***III.- Sobre el caso concreto.*** *En el sub examine, el recurrente asevera que el 9 de junio de 2023 fue publicado el cartel de licitación mayor nro. 2023LY-000025-0001000001: ADQUISICIÓN DE TAGS RFID, EQUIPOS Y SERVICIOS PARA MARCHAMO DIGITAL en el Sistema Integrado de Compras Públicas. Afirma que el objeto de la licitación es la contratación para la compra de "stickers" que contienen un chip de radiofrecuencia RFID; este sería utilizado a partir de 2024 por todos los vehículos en lugar de la actual calcomanía de marchamo. Reclama que tal dispositivo permitirá el rastreo y monitoreo de las personas e incidirá en la protección de datos. Acusa que no existe ley previa que autorice tal proceder, lo que es necesario cuando se trata del derecho a la intimidad (artículo 24 constitucional).*
Ahora bien, la Sala considera que los reclamos planteados no pueden prosperar por varios motivos. ***La Sala destaca que el accionante plantea una situación hipotética, que dista de ser una amenaza cierta, actual e inminente contra derechos fundamentales*** *(véase, verbigracia, la resolución nro. 2018-017621 de las 10:10 horas del 23 de octubre de 2018).* ***Si se obviara este obstáculo procesal, el recurso tampoco encontraría acogida en la Sala, toda vez que los informes rendidos desvirtúan los planteamientos del accionante****. Así, en lo que respecta al rastreo y monitoreo de las personas, se tuvo por probado que la contratación versa sobre etiquetas RFID pasivas, que no permiten trazar la trayectoria de un vehículo ni establecer la posición de un vehículo en un conjunto de lecturas sucesivas. No cuentan con un sistema de referencia de posición global. En cuanto a la información que incluiría la etiqueta RFID, se indicó que sería la misma que contiene el actualmente el marchamo físico (información que está disponible para cualquier persona que lea la calcamonía que se pega en el parabrisas del vehículo). Además, el acceso a la información de la etiqueta RFID requeriría un dispositivo especial, homologado por la SUTEL, por lo que se resguardaría del uso no autorizado (…)"* (El destacado no forma parte del original).

D. Inexistencia de gestiones sin atender. En el escrito de interposición de este amparo, el tutelado señala que desconoce varios aspectos relacionados con la instalación y uso de la aplicación de doble factor de autenticación en cuestión y reclama que SUTEL ha omitido pronunciarse al respecto. Asimismo, señala que el Consejo de SUTEL no ha emitido un pronunciamiento expreso sobre los motivos por los cuales no se considera su propuesta (en cuanto a utilizar otro mecanismo de autenticación). No obstante, estos argumentos no son de recibo, en el tanto el recurrente no señaló o alegó que un determinado día haya presentado alguna gestión ante la recurrida relacionada con tales temas. Tampoco, aportó prueba alguna sobre el particular. Cabe agregar que la única gestión planteada (recurso de reconsideración y solicitud de medica cautelar), fue resuelta incluso antes de notificado este amparo a la parte recurrida.

E. Sobre la presunta sanción impuesta. En cuanto a este agravio, conviene señalarle al tutelado que, a la luz de las argumentaciones *supra* señaladas y explicadas en este considerando, no observa la Sala que el hecho de haberse señalado su nombre como parte de las personas que se opusieron a instalar la aplicación bajo estudio se pueda traducir en una medida arbitraria, irrazonable o desproporcionada. Recuérdese que, según lo expuesto, la medida se tomó por motivos de seguridad institucional y, además, no representa ninguna amenaza o violación a la intimidad y privacidad del funcionario (al desacreditarse el acceso a sus datos personales).
De todos modos, conviene aclararle al tutelado que, en caso de considerar que fue sancionado en calidad de funcionario público y no se respetó, al efecto, el debido proceso, debe acudir ante la jurisdicción laboral a formular el reclamo que considere pertinente. En ese particular, en la Sentencia No. 2025-3678 de las 09:20 hrs. de 7 de febrero de 2025 este Sala dispuso lo siguiente:
"(…) cuando quien recurre ante la Sala Constitucional para atacar presuntas violaciones al debido proceso constitucional, es funcionario o servidor público, como ocurre en este caso, debe hacérsele saber que en lo tocante a supuestos quebrantos sustanciales al debido proceso en la función pública, los servidores afectados deben acudir ante la jurisdicción laboral, toda vez que, ante la promulgación de la Reforma Procesal Laboral, Ley N° 9343 de 25 de enero de 2016 —que está vigente desde el 25 de julio de 2017—, esta Sala, en sentencia N° 2017-017948 de las 9:15 horas del 8 de noviembre de 2017, indicó lo siguiente: "(…) Ciertamente, la tutela de la Sala Constitucional, en tratándose de la materia laboral, deriva de la aplicación del Título V, Capítulo Único, de la Constitución Política, denominado Derechos y Garantías Sociales. Es allí, donde encuentran protección constitucional, por medio del recurso de amparo, el derecho al trabajo, al salario mínimo, a la jornada laboral, al descanso semanal, a vacaciones anuales remuneradas, a la libre sindicalización, al derecho de huelga, a la celebración de convenciones colectivas de trabajo, entre otros; todo ello, con ocasión del trabajo. Sin embargo, bajo una nueva ponderación, dada la promulgación de la Reforma Procesal Laboral, Ley N° 9343 de 25 de enero de 2016, vigente desde el 25 de julio de 2017, esta Sala considera que ahora todos los reclamos relacionados con esos derechos laborales, derivados de un fuero especial (por razones de edad, etnia, sexo, religión, raza, orientación sexual, estado civil, opinión política, ascendencia nacional, origen social, filiación, discapacidad, afiliación sindical, situación económica, así como cualquier otra causal discriminatoria contraria a la dignidad humana), tienen un cauce procesal expedito y célere, por medio de un proceso sumarísimo y una jurisdicción plenaria y universal, para su correcto conocimiento y resolución, en procura de una adecuada protección de esos derechos y situaciones jurídicas sustanciales, con asidero en el ordenamiento jurídico infra constitucional, que tiene una relación indirecta con los derechos fundamentales y el Derecho de la Constitución. Iguales razones caben aplicar para las personas servidoras del Estado, respecto del procedimiento ante el Tribunal de Servicio Civil que les garantiza el ordenamiento jurídico, así como las demás personas trabajadoras del Sector Público para la tutela del debido proceso o fueros semejantes a que tengan derecho de acuerdo con el ordenamiento constitucional o legal. En fin, el proceso sumarísimo será de aplicación, tanto del sector público como del privado, en virtud de un fuero especial, con goce de estabilidad en el empleo o de procedimientos especiales para su tutela, con motivo del despido o de cualquier otra medida disciplinaria o discriminatoria, por violación de fueros especiales de protección o de procedimientos, autorizaciones y formalidades a que tienen derecho, las mujeres en estado de embarazo o periodo de lactancia, las personas trabajadoras

adolescentes, las personas cubiertas por el artículo 367, del Código de Trabajo, las personas denunciantes de hostigamiento sexual, las personas trabajadoras indicadas en el artículo 620, y en fin, de quienes gocen de algún fuero semejante mediante ley, normas especiales o instrumentos colectivos de trabajo. Esta nueva legislación incorpora, en el ordenamiento jurídico, una serie de novedosos mecanismos procesales: como plazos más cortos para la realización de los actos procesales, una tutela jurisdiccional más eficaz, asistencia legal gratuita, implementa la oralidad en los procedimientos; y, como consecuencia, incluye los sub-principios de concentración, inmediación y celeridad, tasa de forma expresa las situaciones en las que cabe ejercer los medios de impugnación, entre otros institutos, todo lo cual tiende a la realización de una eficaz tutela judicial en materia laboral, como garantía de protección de los derechos laborales constitucionales, dadas las nuevas características de simplicidad, celeridad y prontitud de los procesos laborales, lo que constituye una mayor garantía para la efectiva protección de las situaciones jurídicas sustanciales que involucren aspectos laborales y en las que, para su debida tutela, se requiera recabar elementos probatorios o zanjar cuestiones de mera legalidad. De modo, que las pretensiones deducidas en este recurso de amparo, son propias de ser conocidas a través de los nuevos mecanismos procesales que prevé la citada Reforma Procesal Laboral o, en su caso, ante la jurisdicción de lo contencioso administrativo, de conformidad con lo resuelto por esta Sala en la Sentencia N° 2008-002545 de las 8:55 horas del 22 de febrero de 2008, motivo por el cual, lo procedente es rechazar de plano el recurso y remitir a la parte interesada a la jurisdicción competente, para que sea allí donde reciba, en forma plena, la tutela judicial que pretende (…)".

F. Teletrabajo como herramienta opcional para el recurrente. Finalmente, es importante tomar en cuenta –tal y como informó la autoridad recurrida– que la implementación del doble factor de autenticación en el dispositivo móvil propiedad de un funcionario de la SUTEL no es una obligación impuesta ni obstaculiza su trabajo, sino que es una medida de seguridad que deben implementar, únicamente, si desean laborar en la modalidad de teletrabajo. En ese sentido, es claro que, si no desean instalar la herramienta en análisis en sus dispositivos móviles, los funcionarios (como es el caso del recurrente), tienen la posibilidad de realizar sus labores de forma presencial en las oficinas de la SUTEL.

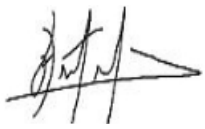
***

Bajo dicha inteligencia, al descartarse quebranto alguno a los derechos fundamentales del recurrente, lo que procede es desestimar el presente proceso de amparo.

V.- DOCUMENTACIÓN APORTADA AL EXPEDIENTE. Se previene a las partes que de haber aportado algún documento en papel, así como objetos o pruebas contenidas en algún dispositivo adicional de carácter electrónico, informático, magnético, óptico, telemático o producido por nuevas tecnologías, estos deberán ser retirados del despacho en un plazo máximo de 30 días hábiles contados a partir de la notificación de esta sentencia. De lo contrario, será destruido todo aquel material que no sea retirado dentro de este plazo, según lo dispuesto en el "Reglamento sobre Expediente Electrónico ante el Poder Judicial", aprobado por la Corte Plena en sesión número 27-11 del 22 de agosto de 2011, artículo XXVI y publicado en el Boletín Judicial número 19 del 26 de enero de 2012, así como en el acuerdo aprobado por el Consejo Superior del Poder Judicial, en la sesión número 43-12 celebrada el 3 de mayo de 2012, artículo LXXXI.

POR TANTO:

Se declara sin lugar el recurso.-

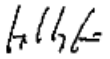


Fernando Castillo V.
Presidente

Fernando Cruz C.

Paul Rueda L.

Luis Fdo. Salazar A.



Jorge Araya G.

Anamari Garro V.

Ingrid Hess H.

Documento Firmado Digitalmente

Teléfonos: 2549-1500 / 800-SALA-4TA (800-7252-482). Fax: 2220-4607 / 2220-4844. Dirección electrónica: www.poder-judicial.go.cr/salaconstitucional. Dirección: (Sabana Sur, Calle Morenos, 100 mts. Sur de la iglesia del Perpetuo Socorro).