CAJA COSTARRICENSE DE SEGURO SOCIAL
Auditoría Interna
Teléfono: 2539-0821 ext. 2000-7468
Correo electrónico: coinccss@ccss.sa.cr

Al contestar refiérase a: **ID-141709**

AS-ATIC-0074-2025
9 de julio de 2025

Máster
Robert Picado Mora, subgerente
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES - 1150

Máster
Natalia Villalobos Leiva, subdirectora
DIRECCIÓN ADMINISTRACIÓN Y GESTIÓN DE PERSONAL - 1131

Estimado(a) señor(a):

ASUNTO: **Oficio de Asesoría sobre medidas de ciberseguridad en teletrabajo conforme a lineamientos del MIDEPLAN y MICITT (2 de julio de 2025)**

En cumplimiento de las actividades preventivas consignadas en el Plan Anual Operativo de esta Auditoría, para el período 2025 y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, se presentan consideraciones para robustecer la infraestructura y los controles asociados a la ciberseguridad.

Lo anterior se sustenta en la información conocida por esta Auditoría, a partir del lineamiento "Gobierno refuerza medidas de ciberseguridad en el teletrabajo para proteger información institucional"[1], publicado el 2 de julio del 2025 en el sitio web oficial del Ministerio de Planificación Nacional y Política Económica (MIDEPLAN).

A ese respecto, la instrucción está dirigida a todas las instituciones del Estado, con el objetivo de que realicen una revisión integral de los servicios de acceso remoto mediante redes privadas virtuales (VPN[2]) en entornos de teletrabajo.

1. OBSERVACIONES

En este contexto, y conforme a lo señalado en la disposición, su propósito es fortalecer los mecanismos de protección digital frente a un entorno caracterizado por riesgos crecientes, reafirmando así el compromiso del Gobierno con la seguridad de la información y la continuidad operativa de las instituciones públicas.

Como parte de esta responsabilidad, la Caja Costarricense de Seguro Social (CCSS) no está exenta y debe velar por minimizar la exposición a incidentes de ciberseguridad, tales como: accesos no autorizados, suplantación de identidad o interrupciones en servicios críticos, entre otras amenazas que podrían derivarse de configuraciones inadecuadas o de la ausencia de controles eficaces.

Por ello, la adopción de estándares, como los mencionados en la disposición supracitada, así como otros de mayor rigurosidad en materia de ciberseguridad, no solo fortalece la protección de los datos institucionales (independientemente de su lugar de uso y medio), sino que también habilita, de forma segura, la implementación de modalidades laborales como el teletrabajo.

[1] https://www.mideplan.go.cr/gobierno-refuerza-medidas-de-ciberseguridad-en-el-teletrabajo-para-proteger-informacion
[2] Una VPN (Virtual Private Network) o Red Privada Virtual es una tecnología que permite establecer una conexión segura y cifrada entre un dispositivo (como una computadora, teléfono o tablet) y una red, a través de Internet.

A continuación, se presentan las observaciones pertinentes sobre el tema:

- Para dar cumplimiento a lo establecido en la instrucción emitida por el Gobierno, es fundamental contar con **documentos claros y actualizados que definan las responsabilidades de todas las personas involucradas en la gestión tecnológica y de ciberseguridad señaladas en la publicación**, con el fin de evitar ambigüedades sobre las funciones y obligaciones de cada rol dentro de la CCSS, considerando las condiciones actuales.

  En este contexto, resulta imprescindible que la Dirección de Tecnologías de Información y Comunicaciones, la Dirección de Administración y Gestión de Personal, entre otras instancias de negocio correspondientes, revise, refuerce o actualice los criterios técnicos vigentes en la materia.

  Esta labor puede incluir tanto la socialización y reafirmación de los lineamientos ya establecidos como la actualización de la guía técnica existente, incorporando mejoras que permitan responder eficazmente a los nuevos desafíos operativos y tecnológicos.

- Se debe verificar que los servicios tecnológicos cuenten obligatoriamente con mecanismos de autenticación multifactor (2FA) y restricciones de acceso basadas en geolocalización, permitiendo únicamente conexiones originadas dentro del territorio nacional.

  Para ello, será fundamental realizar un análisis de los aspectos mencionados y **certificar ante las instancias gubernamentales correspondientes el cumplimiento de dichos requisitos**. Asimismo, resulta conveniente **comunicar al grupo de involucrados y/o usuarios de los servicios TIC, sobre las condiciones tecnológicas del servicio utilizado.**

- El comunicado recuerda que, durante la modalidad de teletrabajo, está estrictamente prohibido el uso de redes Wi-Fi públicas, debido al alto riesgo para la seguridad de la información institucional.

  En este sentido, es necesario **aplicar las configuraciones técnicas para mitigar estos riesgos**, preferiblemente de manera institucional y controlada. No obstante, también es esencial que los usuarios comprendan el propósito de estas restricciones y los beneficios asociados con la seguridad general de la organización.

- Adicionalmente, la publicación enfatiza sobre la posible peligrosidad de la conexión de computadoras personales a las redes informáticas de la institución. Por ello, el uso de dispositivos sin los estándares requeridos podría comprometer la integridad, disponibilidad y confidencialidad de los sistemas institucionales; práctica que no se limita únicamente a la modalidad de teletrabajo, sino a la aplicación general de cualquier entorno donde se desarrollen funciones institucionales.

  El objetivo principal es evitar el uso de equipos personales (como computadoras, tabletas, teléfonos móviles u otros dispositivos) que no cuenten con las condiciones mínimas de seguridad ni con las características técnicas adecuadas. En este sentido, resulta fundamental que el ente rector en tecnologías de información defina, actualice y comunique de manera oportuna los requisitos que deben cumplirse en caso de que se autorice el uso de equipos personales, a fin de mitigar riesgos y garantizar la protección de la información institucional.

  Incluso, debe ser analizada la posibilidad de establecer un protocolo y/o acuerdo formal mediante el cual el funcionario acepte expresamente las condiciones de uso de su dispositivo personal, comprometiéndose a cumplir con los controles de seguridad definidos.

En este sentido, debe quedar claro que esta medida no busca cuestionar el compromiso ni la disposición del personal para contribuir con la institución. Por el contrario, responde a la necesidad de canalizar ese aporte dentro de un marco orientado a garantizar la protección de los activos tecnológicos y la salvaguarda de la información crítica, siempre bajo condiciones que no comprometan la seguridad institucional.

- Con respecto a la suspensión del teletrabajo en aquellas instituciones que no han cumplido con las medidas de seguridad estipuladas, establece: una vez implementadas dichas medidas, las instituciones estarán en capacidad de restablecer este beneficio, debiendo para ello notificar formalmente a la Dirección de Ciberseguridad del MICITT el cumplimiento de los requerimientos técnicos correspondientes.

  Frente a este escenario, no solo es importante conocer el procedimiento para restablecer el teletrabajo, sino que **resulta indispensable aplicar políticas estrictas y centralizadas sobre el uso de equipos y servicios tecnológicos.** Estas políticas deben entenderse como configuraciones técnicas definidas a nivel organizacional, que establecen con claridad lo permitido o restringido en los dispositivos conectados a la red institucional. Su implementación, idealmente mediante herramientas de gestión centralizada, permite ejercer una gobernanza efectiva sobre los entornos tecnológicos, garantizando equipos monitoreados, generación de alertas preventivas cuando sea necesario, y minimización de la exposición a riesgos de ciberseguridad.

  Esto implica asegurar que los dispositivos utilizados se mantengan actualizados, cuenten con los aplicativos corporativos requeridos y cumplan con las medidas mínimas de seguridad, evitando así cuestionamientos sobre la solidez de la infraestructura tecnológica institucional.

2. CONSIDERACIONES NORMATIVAS

Entre los principales aspectos normativos vinculados a esta temática se encuentra la Ley No. 9738, publicada el 30 de setiembre del 2019 en el Diario Oficial La Gaceta (Alcance No. 211), así como su Reglamento (No. 42083-MP-MTSS-MIDEPLAN-MICITT), los cuales establecen el marco legal para promover, regular e implementar el teletrabajo como una herramienta para la modernización organizacional y la generación de empleo, mediante el uso de tecnologías de la información y la comunicación.

Por otra parte, la Ley General de Control Interno No. 8292, en el Artículo N°10- “Responsabilidad por el sistema de control interno”, hace referencia a lo siguiente:

> *“Artículo 10 Responsabilidad por el sistema de control interno.*
>
> *Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento.”*

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, versión 2.0, 2022 emitidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, MICITT, señalan en el apartado XI. Seguridad y Ciberseguridad, lo siguiente:

"La institución debe tener y aplicar en forma consistente una estructura formal al nivel institucional, que permita establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados.

Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos contractuales adquiridos por la institución.

La Institución, basada en la Política de seguridad de información / ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.

La Institución debe propiciar un ambiente seguro, considerando la seguridad física, lógica y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.

La Institución debe establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.

La institución debe implementar medidas de control asociadas a la administración del riesgo de seguridad de la información y ciberseguridad, que permitan el cumplimiento de los objetivos de los procesos, protegiendo la confidencialidad, autenticidad, privacidad e integridad de la información.

La Institución debe realizar una valoración de controles a implementar a través de una declaración de aplicabilidad, que permita contrarrestar los riesgos de seguridad de la información, incluyendo una valoración de madurez (medidas organizativas, técnicas o legales que se aplican) Así mismo, establecer e implementar los mecanismos que permitan contrastar los controles definidos contra los controles que se están aplicando."

CONSIDERANCION FINAL

La ciberseguridad es un pilar fundamental para la protección de los activos digitales de una organización, incluyendo datos sensibles, infraestructura tecnológica y sistemas críticos. En un entorno cada vez más interconectado, las amenazas cibernéticas representan riesgos reales que pueden comprometer la confidencialidad, integridad y disponibilidad de la información, afectando directamente la continuidad operativa y la confianza de los usuarios o clientes.

En ese sentido, es indispensable disponer de medidas de ciberseguridad sólidas que permitan prevenir, detectar y responder eficazmente ante incidentes. Estas acciones no solo protegen la información institucional y evitan pérdidas económicas, legales o reputacionales, sino que también aseguran el cumplimiento de normativas y estándares internacionales, integrando la ciberseguridad como parte esencial de la gestión moderna de riesgos.

La ciberseguridad debe aplicarse de forma transversal en todos los entornos donde se desarrolla la tecnología, como el teletrabajo, el uso de servicios en la nube, aplicaciones móviles o dispositivos conectados (IoT). En estos escenarios, garantizar conexiones seguras, el uso de dispositivos protegidos y una adecuada gestión de accesos es indispensable para asegurar operaciones eficientes y seguras, sin comprometer la infraestructura institucional.

Consecuentemente, los recursos tecnológicos (ya sea en modalidad presencial o remota) deben estar sujetos a medidas como las mencionadas en las observaciones previas: documentación clara sobre roles y responsabilidades, criterios técnicos definidos por el ente rector en TIC, y una coordinación efectiva entre las áreas técnicas (CGI), las unidades de negocio y los usuarios finales.

Como resultado, es fundamental que todos los actores trabajen en conjunto para identificar situaciones que puedan poner en riesgo la infraestructura tecnológica, así como para establecer procedimientos claros de revisión y mitigación. La colaboración entre áreas técnicas y usuarios permite una respuesta ágil y efectiva ante posibles vulnerabilidades.

A raíz de esto, la aplicación de políticas estrictas y medidas robustas que garanticen el cumplimiento de las disposiciones vigentes y de las mejores prácticas en ciberseguridad será siempre un factor clave de éxito. En los casos en que no se cumplan los requisitos establecidos, se deberá actuar de forma diferenciada, ya sea excluyendo temporalmente los equipos que representen un riesgo o gestionando estrategias priorizadas de mitigación.

Estas acciones aplican tanto a servicios esenciales, como no esenciales, ya que cualquier falla en la seguridad puede comprometer directamente los servicios que brinda la CCSS en áreas críticas como salud, pensiones y recaudación patronal.

Por tanto, es fundamental que la institución aproveche al máximo las herramientas tecnológicas disponibles para el monitoreo del estado de los equipos, especialmente en aspectos clave como: obsolescencia tecnológica; cumplimiento de normas de seguridad; vigencia del versionamiento del sistema operativo; aplicación de actualizaciones; mejoras y parches de seguridad; entre otros elementos que forman parte integral de la postura institucional en ciberseguridad.

Finalmente, resaltar la importancia de impulsar el uso de procesos automatizados como primera línea de defensa. En aquellos casos que requieran intervención manual, es necesario implementar mecanismos de supervisión estrictos que aseguren el cumplimiento de las condiciones técnicas requeridas, garantizando así una infraestructura tecnológica segura, resiliente y alineada con los objetivos institucionales.

Por todo lo anterior, y en el marco de una gestión responsable de los riesgos tecnológicos, se presenta a conocimiento de la Administración Activa, lo expuesto en este oficio de asesoría, con el fin de aportar elementos de juicio que respalden la toma de decisiones estratégicas en materia de ciberseguridad.

Por ello, la implementación de medidas robustas y sostenibles, como las promovidas por el Gobierno e identificadas a nivel interno como oportunidades de mejora, no solo fortalece la postura institucional frente a amenazas cibernéticas emergentes, sino que también garantiza la continuidad de los servicios, protege los activos críticos y fomenta una cultura organizacional orientada a la prevención, la resiliencia y el cumplimiento normativo. En este sentido, se recomienda valorar integralmente las observaciones planteadas, de manera que las decisiones y acciones adoptadas se alineen con los principios de legalidad, eficiencia, eficacia, transparencia y satisfacción del interés público.

Atentamente,

AUDITORÍA INTERNA

Firmado Digitalmente

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

C: Licenciada Mónica Taylor Hernández, presidente, Presidencia Ejecutiva - 1102
Doctora Jenny Madrigal Quirós, jefe de despacho, Gerencia General -1100
Doctor Alexander Sánchez Cabo, gerente a.i. Gerencia Médica-2901
Licenciado Gustavo Picado Chacón, gerente, Gerencia Financiera -1103
Máster Gabriela Artavia Monge, gerente a.i., Gerencia Administrativa-1104
Doctor Esteban Vega de la O, gerente, Gerencia Logística -1106
Ingeniero Jorge Granados Soto, gerente, Gerencia Infraestructura y Tecnologías -1107
Licenciado Jaime Barrantes Espinoza, gerente Gerencia Pensiones-9108
Auditoría Interna 1111

Referencia: ID-141709