MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE SALUD Y PROTECCIÓN SOCIAL
BOGOTÁ, MAYO DE 2025

TABLA DE CONTENIDO

1. OBJETIVO

Establecer un marco integral de políticas de seguridad de la información para el Ministerio de Salud y Protección Social, garantizando el cumplimiento riguroso de los principios fundamentales de confidencialidad, integridad y disponibilidad de la información. Este marco se fundamentará en la Norma ISO 27001:2022, para las mejores prácticas, promoviendo así la protección efectiva de los activos de información y la gestión proactiva de riesgos asociados a la seguridad de la información.

2. ALCANCE

Comienza con la definición detallada de las políticas de seguridad, abarcando principios, directrices y normas aplicables, continua con el establecimiento de la estructura organizativa mediante la asignación de roles y responsabilidades específicas para la gestión de la seguridad de la información, asegurando que los servidores públicos del Ministerio comprendan su papel en la protección de los activos de información, y finaliza con la descripción de los lineamientos necesarios para cumplir con los requisitos normativos y regulatorios relacionados con la seguridad de la información.

3. ÁMBITO DE APLICACIÓN

Las disposiciones contenidas en este Manual están dirigidas a salvaguardar la información gestionada y administrada por el Ministerio de Salud y Protección Social. Estas políticas deben ser adoptadas y cumplidas por todos los funcionarios, contratistas, proveedores y terceros que se vean involucrados con el uso de los activos de información, así como, los servicios de tecnologías de la información y las comunicaciones ofrecidos por el Ministerio.

Además, el alcance de este Manual se extiende a todos los procesos del Ministerio que forman parte del Sistema Integrado de Gestión, asegurando así, una implementación coherente y efectiva de las políticas de seguridad de la información en toda la Entidad.

4. DOCUMENTOS ASOCIADOS AL MANUAL

Los siguientes documentos hacen parte integral, entre otros, del Sistema de Gestión de Seguridad de la Información del Ministerio de Salud y Protección Social, los cuales pueden ser consultados en la intranet, en el siguiente link: https://migestion.minsalud.gov.co/suiteve/base/client?soa=6&_sveVrs=1002820240831&

- ASIC01 Sistema de gestión y mejoramiento institucional.
- ASIG01 Guía para la Administración Integral de riesgos en los procesos.
- ASIG02 Guía para la medición de la eficacia del SGSI.
- ASIG03 Guía para el levantamiento y valoración de activos de seguridad información.
- ASIG04 Guía de uso y protección de firmas electrónicas.
- ASIG05 Gestión incidentes seguridad información
- ASIG06 Metodología de elaboración y control de documentos y registros.
- ASIG07 Solicitud de certificados de sitio seguro
- ASIG08 Guía de administración de usuarios
- ASIG09 Guía para el teletrabajo y trabajo remoto
- ASIP05 Administración del sistema integrado de gestión y MIPG.
- ASIM02 Manual de políticas de seguridad de la información.
- ASIM03 Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG – SST).
- ASIM04 Manual del Sistema de Gestión de Seguridad en la Información.
- ASIS02 Declaración de aplicabilidad.

- ASIS03 Normatividad en Seguridad de la Información.
- ASIS04 Política de privacidad y protección de datos del MSPS.
- ASIS05 Política general Seguridad de la Información.
- ASIS06 Política de Administración de Riesgos Institucionales.
- ASIS09 Política Ambiental del Ministerio de Salud y Protección

5. NORMATIVA Y OTROS DOCUMENTOS EXTERNOS

Por la importancia y la necesidad de adoptar medidas y controles para proteger la seguridad de la información, se hace necesario tener en cuenta la normatividad existente y relacionada con este tema, por lo que se toma en consideración la referida en el siguiente documento soporte: Ver documento soporte ASIS03 Normatividad en Seguridad de la Información.

6. Reviste particular importancia la Ley Estatutaria 1581 de 2012, sus Decretos Reglamentarios y la Circular externa 02 de 2024. del 21 de agosto de 2024 "Lineamientos sobre el Tratamiento de Datos personales en Sistemas de Inteligencia Artificial "DEFINICIONES[1]

Los conceptos y definiciones que a continuación se referencian hacen parte fundamental y necesaria para la comprensión del presente documento, para lo cual, se relacionan los siguientes:

Activo: cualquier cosa que tiene valor para la organización. [ISO/IEC 2382:2015]

Activo de información: cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. [INCIBE]

Amenaza: posible violación de la seguridad informática. [ISO/IEC 2382:2015]

Análisis de riesgo: Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo [INCIBE].

Antivirus: Software de protección para evitar que ejecutemos algún tipo de software malicioso en nuestro equipo que infecte al equipo. [INCIBE]

Doble factor de autenticación (2FA): se habla de doble factor de autenticación cuando un sistema de autenticación utiliza por lo menos dos de los tres factores básicos de autenticación: Algo que la persona sabe (contraseña, PIN, número de un documento personal, nombre de algún pariente, etc.) Algo que la persona posee (credencial, tarjeta magnética, token, etc.) o algo que la persona es (reconocimiento facial, voz, iris, retina, etc.). De este modo, si uno de los factores se ve comprometido, todavía existe un segundo factor que garantiza la seguridad.[2]

Backup: copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados. [INCIBE]

[1] Estas definiciones se enmarcan en la ISO 27000
[2] Control 5.15 Control de Acceso a Sistemas y Aplicaciones ISO 27001:2022

Comunicación y consulta de riesgos: Conjunto de procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información y entablar un diálogo con las partes interesadas con respecto a la gestión del riesgo.[3]

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados[4].

Criptografía: es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado. [INCIBE].

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos - y su justificación, así como la justificación de las exclusiones de controles del anexo A de la ISO 27001.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[5].

Evaluación del riesgo: Proceso global de identificación, análisis y estimación de riesgos[6].

Evento de seguridad de la información: Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad[7].

Gestión el riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo[8].

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información[9].

Identificación del Riesgo: proceso para encontrar, reconocer y describir riesgos[10].

Impacto: El costo para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.[11]

---

[3] La ISO/IEC 27000, en términos y definiciones 3.65 (que trata sobre Acciones para abordar riesgos y oportunidades)
[4] La ISO/IEC 27000 define “Confidencialidad” en términos y definiciones 3.10 como Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.
[5] En la ISO/IEC 27000, define “Disponibilidad” en términos y definiciones 3.7 como Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada.
[6] En la ISO/IEC 27000 el término “Evaluación de riesgos de seguridad de la información” se menciona en términos y definiciones 3.64
[7] En la ISO/IEC 27000, el término "Evento de seguridad de la información" se menciona en términos y definiciones 3.30, donde se define como cualquier ocurrencia identificada que podría afectar la seguridad de la información.
[8] En la ISO/IEC 27000, se define el término “Gestión de riesgos” en términos y definiciones 3.69
[9] La ISO/IEC 27000 define “Incidente de seguridad de la información” en términos y definiciones 3.31
[10] En la ISO/IEC 27000 el término “Evaluación de riesgos de seguridad de la información” se menciona en términos y definiciones 3.68
[11] Características del impacto en seguridad de la información: consecuencias en confidencialidad, integridad y disponibilidad: https://www.pmg-ssi.com/2015/04/iso-27001-el-impacto-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion/#:~:text=Caracter%C3%ADsticas%20del%20impacto,despu%C3%A9s%20de%20materializar%20las%20amenazas.

Integridad: Propiedad de la información relativa a su exactitud y completitud[12].

MSPS: sigla del Ministerio de Salud y Protección Social.

OTIC: sigla de la Oficina de Tecnología de la Información y las Comunicaciones perteneciente al Ministerio de Salud y Protección Social.

Política de seguridad: son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos. [INCIBE].

Probabilidad: Posibilidad de que ocurra algo[13].

Programas Utilitarios: Los programas utilitarios son programas que brindan una "utilidad" específica y no están diseñados para un tipo de usuario particular[14].

Riesgo: El riesgo a menudo se caracteriza por la referencia a posibles "eventos" y "consecuencias" o una combinación de estos[15].

Seguridad de la información[16]: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.

Sistema de gestión de la seguridad de la información[17]: SGSI Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora.

Tratamiento de Riesgos[18]: proceso de modificar el riesgo, mediante la implementación de controles.

Usuario[19]: todo servidor público, contratista, ente regulador, socios de negocios, y terceros entre otros que estén involucrados con información del Ministerio de Salud y Protección Social.

Valor del Impacto[20]: está determinado por el responsable del activo de información, quién provee cuanto se vería afectado por incidentes de los activos a cargo.

---

[12] En la ISO/IEC 27000 el término "Integridad" se menciona en términos y definiciones 3.36
[13] En la ISO/IEC 27000 el término "Probabilidad" se menciona en términos y definiciones 3.40
[14] Los programas utilitarios resuelven problemas de administración del sistema del equipo de cómputo: https://sigi.sic.gov.co/SIGI/portal/view_term.php?idTermino=573#:~:text=Son%20programas%20dise%C3%B1ados%20para%20realizar,sistema%20del%20equipo%20de%20c%C3%B3mputo.
[15] En la ISO/IEC 27000 el término "Riesgo" se menciona en términos y definiciones 3.61
[16] En la ISO/IEC 27000 el término "Seguridad de la Información" se menciona en términos y definiciones 3.28
[17] SGSI**:** Sistema que gestiona la seguridad de la información a través de políticas y procesos de control. (ISO 27001:2022-clàusula 3.14)
[18] **Tratamiento de Riesgos**: Proceso para modificar riesgos mediante controles adecuados y efectivos. (ISO 27001:2022- cláusula 6.1.2)
[19] **Usuario**: Cualquier persona o entidad que interactúa con la información del Ministerio. (ISO 27001:2022- cláusula 5.1;7.2)
[20] **Valor del Impacto**: Grado de afectación de un activo ante incidentes, determinado por su responsable. (ISO 27001:2022-clàusula 6.1.2)

Vulnerabilidad[21]**:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7. INTRODUCCIÓN

El Ministerio de Salud y Protección Social (MSPS), en cumplimiento de lo establecido por la norma técnica sobre seguridad de la información (ISO 27001:2022), que define la preservación de la confidencialidad, integridad y disponibilidad de la información, reconoce la imperante necesidad de proteger, conservar y asegurar los activos de información que gestiona. En este contexto, el MSPS ha establecido un Sistema de Gestión de Seguridad de la Información (SGSI) que incluye medidas de control, así como un conjunto de reglas, normas y protocolos de actuación dirigidos a gestionar los riesgos asociados a la seguridad de la información a los que puede estar expuesto el Ministerio.

En consecuencia, este manual establece las políticas que integran el SGSI, las cuales deben ser adoptadas y aplicadas por todos los servidores públicos, contratistas, terceros vinculados al Ministerio y proveedores, sin distinción alguna en relación con su situación contractual, dependencia en la que presten servicios, nivel de tareas desempeñadas o funciones definidas a través de contratos o acuerdos laborales.

Las políticas de seguridad aquí establecidas están alineadas con la normativa legal colombiana vigente y las mejores prácticas en seguridad de la información, fundamentadas en la norma ISO 27001:2022 y el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

8. VIGENCIA Y ACTUALIZACIÓN DE LAS POLÍTICAS

El Manual de Políticas de Seguridad de la Información será objeto de actualización en respuesta a cambios significativos en el entorno del Ministerio o conforme a las directrices gubernamentales aplicables.

Las revisiones considerarán diversos factores, tales como: incidentes de seguridad, vulnerabilidades identificadas, modificaciones en la infraestructura organizacional o tecnológica, así como cambios en los procesos y en los objetivos estratégicos del Ministerio.

Este enfoque garantiza que las políticas sean pertinentes y efectivas frente a un entorno en constante evolución y a las amenazas emergentes en el ámbito de la seguridad de la información.

9. APLICACIÓN, CONTRAVENCIONES Y EXCEPCIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información son de cumplimiento obligatorio en todos los niveles, por lo tanto, todos los servidores públicos, contratistas y terceros que interactúen con el Ministerio de Salud y Protección Social deberán adherirse a lo establecido en el Manual de Políticas de Seguridad de la Información.

En caso de que se evidencie una transgresión o incumplimiento de cualquier política contemplada en este documento, se considerará como una falta disciplinaria, lo que dará inicio a las investigaciones internas pertinentes. Se aplicarán las

[21] **Vulnerabilidad**: Debilidad en un activo que puede ser explotada por amenazas. (ISO 27001:2022-clàusula 6.1.2; 8.1)

sanciones estipuladas en el Régimen Disciplinario aplicable o en el Código General Disciplinario, conforme al proceso GYPC01, que regula la gestión y prevención de asuntos disciplinarios para el MSPS.

Cualquier excepción a lo dispuesto en estas políticas deberá ser evaluada por el Grupo de Seguridad de la Información e Innovación, así como con la aprobación del Comité Institucional de Gestión y Desempeño - CIGD del Ministerio o del Líder de Seguridad de la Información, según corresponda.

Cualquier asunto relacionado con la seguridad de la información del Ministerio que no esté definido por estas políticas deberá ser registrado y sometido a revisión para tomar decisiones adecuadas. El propietario de los activos de información, en coordinación con el Grupo de Seguridad de la Información e Innovación s, evaluará el impacto de las actividades a realizar antes de adoptar cualquier decisión respecto a procedimientos, prácticas, acciones, conceptos o controles relacionados con la seguridad de la información del Ministerio.

10. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas de seguridad de la información se desarrollan teniendo como referencia las buenas prácticas definidas en el Modelo de Seguridad y Privacidad de la Información (MSPI), establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Estas políticas se fundamentan en los principios de seguridad de la información y en los requisitos establecidos en la Declaración de Aplicabilidad del Anexo A de la norma ISO 27001:2022, y aceptados por el Ministerio de Salud y Protección Social (MSPS).

10.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS

La presente política es aplicable a todos los servidores públicos, contratistas y terceros que mantengan una relación directa con el Ministerio de Salud y Protección Social (MSPS), con el objetivo de preservar la seguridad de la información en la Entidad y controlar posibles vulnerabilidades que puedan surgir durante las distintas etapas de los proyectos ejecutados por el MSPS que requieran tratamiento de información.

Se deberán cumplir los siguientes lineamientos:

1. La seguridad de la información debe ser integrada en la gestión de cada uno de los proyectos destinados a apoyar los procesos misionales del MSPS, independientemente de su naturaleza. Esto asegura que los riesgos asociados a la seguridad de la información sean identificados y tratados adecuadamente dentro del proyecto, en alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

2. Los responsables de la gestión de proyectos deben evaluar y validar que los objetivos del proyecto no contravengan las políticas de seguridad de la información establecidas por el Ministerio.

3. Los riesgos relacionados con la seguridad de la información deben ser identificados en las primeras etapas del ciclo de gestión del proyecto, permitiendo así una adecuada planificación y mitigación, conforme a las directrices del MSPI.

4. Los supervisores de contratos o responsables de proyectos deberán reportar cualquier evento o riesgo relacionado con la seguridad a través del canal designado (gr.sgsi@minsalud.gov.co) para notificaciones de incidentes de seguridad de la información.

5. Cualquier incumplimiento respecto a los requisitos de seguridad de la información y privacidad de datos personales establecidos para los proyectos deberá ser informado oportunamente por el supervisor del contrato o responsable

del proyecto a las partes interesadas, incluyendo al Grupo de Seguridad de la Información y Protección de Datos Personales del Ministerio, para tomar las acciones necesarias.

6. Los requisitos relacionados con la seguridad de la información y privacidad de datos personales en todos los proyectos deben ser definidos por sus responsables. Estos requisitos deberán ser aceptados e implementados a lo largo del ciclo de vida del proyecto, realizando revisiones periódicas conforme a su complejidad y según lo requiera el supervisor.

10.2. POLÍTICA PARA DISPOSITIVOS MÓVILES

La presente política es aplicable a todos los servidores públicos, contratistas y terceros que mantengan una relación directa con el Ministerio de Salud y Protección Social (MSPS), con el objetivo de preservar la integridad y disponibilidad de la información que, por su rol, hagan uso de dispositivos móviles en la entidad.

Con base en lo anterior, el MSPS establece el uso de dispositivos móviles enfocado en el aseguramiento de la información a través de los siguientes lineamientos:

1. Los funcionarios a quienes se les asigne dispositivos móviles para el desempeño de sus funciones laborales deberán velar por el buen uso de los elementos asignados, asegurando que se utilicen exclusivamente para fines laborales y conforme a las políticas establecidas.

2. La asignación de dispositivos móviles institucionales se realizará de acuerdo con las necesidades específicas de los cargos y roles dentro del Ministerio, garantizando que cada dispositivo esté destinado a un propósito claro y justificado.

3. Los usuarios autorizados para el uso de dispositivos móviles corporativos y/o personales deben cumplir con las reglas generales establecidas en la documentación relacionada con el uso aceptable de activos.

4. Todos los dispositivos móviles, incluidos celulares que almacenen información, deben contar como mínimo con un sistema de autenticación, como un patrón, código de desbloqueo o clave.

5. Los equipos móviles personales o de terceros que se conecten a la red del Ministerio podrán ser monitoreados para prevenir amenazas hacia la infraestructura tecnológica. Los dispositivos catalogados como una posible amenaza serán bloqueados por parte de los administradores de las plataformas de seguridad perimetral.

6. Los equipos personales no recibirán soporte por parte de la Mesa de Servicios para fallas que no estén asociadas a los servicios ofrecidos por la entidad.

7. Los funcionarios son responsables del uso adecuado de los dispositivos móviles en redes seguras y deben garantizar las protecciones necesarias para evitar el acceso o divulgación no autorizada de la información almacenada y procesada.

8. Los servidores públicos y/o contratistas que utilicen dispositivos móviles personales y manejen información del Ministerio son responsables de acatar las medidas de seguridad de la información y privacidad de los datos personales. Además, deben informar oportunamente a su jefe inmediato o supervisor de contrato sobre cualquier incidente o riesgo que afecte la información o los datos del MSPS.

9. Todos los dispositivos móviles en los que se procese, almacenen o transmita información del MSPS deberán aplicar las políticas de seguridad y privacidad correspondientes. Se debe cumplir con las mejores prácticas en ciberseguridad y las regulaciones vigentes sobre protección de datos personales.

10. Se realizarán revisiones periódicas (cada 3 meses), del cumplimiento de esta política, así como del estado y configuración de los dispositivos móviles, ajustando las medidas según sea necesario para responder a nuevas amenazas o cambios en el entorno tecnológico.

10.3. POLÍTICA DE TELETRABAJO

La presente política es aplicable a todos los servidores públicos del Ministerio de Salud y Protección Social (MSPS) que laboren bajo la modalidad de teletrabajo.

El Ministerio de Salud y Protección Social establece los lineamientos del Teletrabajo en el marco de la Ley 1221 de 2008 "*por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones*", el Decreto reglamentario 1227 del 2022 "*Por el cual se modifican los artículos 2.2.1.5.3, 2.2.1.5.5, 2.2.1.5.8 Y 2.2.1.5.9, Y se adicionan los artículos 2.2.1.5.15 al 2.2.1.5.25 al Decreto 1072 de 2015, Único Reglamentario del Sector Trabajo, relacionados con el Teletrabajo*" y la Resolución 196 de 2016 "*Por la cual se institucionaliza el Teletrabajo en forma voluntaria en la modalidad suplementario en las plantas de personal del Ministerio de Salud y Protección Social*" o las normatividades que la modifique o derogue.

1. Responsabilidades del Ministerio de Salud y Protección Social:

   - Proveer a los teletrabajadores los equipos necesarios para la ejecución de sus funciones o autorizar el uso de equipos personales, siempre que se cumplan y acepten los requisitos mínimos de seguridad y privacidad de la información, evaluados por el Grupo de Soporte Informático del Ministerio.

   - El Ministerio será responsable del licenciamiento del software para los equipos portátiles o estaciones de trabajo suministrados a los teletrabajadores, siempre que la entidad provea los medios necesarios.

   - Proveer una conexión segura a través de VPN (Red Privada Virtual), VDI (Infraestructura de Escritorios Virtuales), FTP (Protocolo de Transferencia de Archivos), entre otras tecnologías establecidas por el MSPS.

2. Responsabilidades del Teletrabajador:

   - Hacer uso responsable de los dispositivos utilizados para teletrabajo. En caso de utilizar dispositivos personales, estos deben contar con la aprobación del encargado del proceso de verificación y validación de los requisitos mínimos de seguridad.

   - Informar al Ministerio de manera inmediata en caso de ser víctima de robo o pérdida de información, ya sea por ciberdelincuencia o hurto.

   - Los usuarios autorizados para desarrollar sus funciones mediante teletrabajo son responsables de garantizar que el sistema operativo, software y herramientas ofimáticas necesarias cuenten con las respectivas licencias y actualizaciones de seguridad.

- Está prohibido utilizar redes públicas (como aeropuertos o cafés internet) para realizar actividades laborales o contractuales en las cuales se deba realizar conexiones a la red y/o aplicativos del MSPS.

10.4. POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS

La presente política es aplicable a todos los servidores públicos, contratistas y terceros que mantengan una relación directa con el Ministerio de Salud y Protección Social (MSPS) para el cumplimiento de sus funciones.

El MSPS establece el uso aceptable de los activos enfocado en el aseguramiento y protección de la información a través de los siguientes lineamientos:

1. Asegurar que los activos de información bajo propiedad del Ministerio se encuentren debidamente inventariados y con un responsable asociado. El inventario debe actualizarse periódicamente o cada vez que se presenten cambios significativos en los objetivos estratégicos, procesos o infraestructura que soporta las operaciones de la entidad.

2. Toda la información del MSPS debe ser procesada y almacenada de acuerdo con su nivel de clasificación, garantizando la protección de las propiedades de confidencialidad, privacidad, integridad y disponibilidad por parte de los servidores públicos.

3. Los usuarios no deberán utilizar los servicios de Internet, correo electrónico, repositorios, entre otros, asignados por el MSPS para ver, descargar, guardar, recibir o enviar información que no esté relacionada con las funciones propias de su cargo.

4. La información laboral generada para el Ministerio debe ser almacenada en los repositorios dispuestos por la entidad a través de los servicios tecnológicos. No se permitirá el almacenamiento en medios removibles (como memorias USB o discos duros externos) ni en servicios de nubes públicas que no sean del Ministerio.

5. Los usuarios son responsables de cumplir con los lineamientos básicos para el respaldo de la información institucional establecidos en la Circular Interna N. 019 del 2017.

6. No está permitido conectar equipos portátiles asignados por la entidad a redes públicas (como Wi-Fi abiertas en aeropuertos, Cafés internet o bibliotecas).

7. La información laboral que requiere ser compartida deberá ser almacenada únicamente en la ubicación destinada para tal fin (Nube Corporativa).

8. Todos los servidores públicos, contratistas y terceros deben devolver los activos de información bajo su responsabilidad una vez finalizado el vínculo laboral con el Ministerio.

9. Es responsabilidad de los usuarios proteger sus contraseñas y/o cuentas de usuario, evitando permitir a otras personas su uso bajo ningún concepto, teniendo en cuenta la utilización del doble factor de autenticación (2FA).

10. Todos los funcionarios públicos, contratistas y terceros son responsables del uso adecuado de la información conforme a los derechos de autor y propiedad intelectual. Se reconoce que el MSPS es propietario de la información suministrada para el desarrollo de actividades laborales o contractuales.

11. El desconocimiento e incumplimiento de las políticas de seguridad y privacidad por parte de los funcionarios públicos contratistas y terceros, generará acciones disciplinarias pertinentes a través de la Oficina de Control Interno Disciplinario.

12. En todas las estaciones de trabajo configuradas bajo el dominio del Ministerio no se permite la instalación de software sin previa autorización del responsable del proceso y del Grupo de Seguridad de la Información y Protección de Datos Personales. Los usuarios que requieran software adicional deberán solicitarlo formalmente, justificando su necesidad.

13. Es responsabilidad del encargado del proceso asegurarse que el software instalado cuente con el respectivo licenciamiento para prevenir repercusiones legales y daños técnicos sobre los equipos e infraestructura tecnológica.

14. Se deben validar los riesgos asociados a la migración hacia nuevas versiones del software, así como asegurar el correcto funcionamiento y actualización regular de sistemas y herramientas tecnológicas utilizadas en el Ministerio.

10.5. POLÍTICA DE CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN

La presente política es aplicable a todos los servidores públicos, contratistas y terceros que mantengan una relación directa con el Ministerio de Salud y Protección Social (MSPS), que por su rol manejen, conozcan o tengan bajo su responsabilidad o custodia información del Ministerio.

Dando cumplimiento a lo establecido por la Ley de Transparencia 1712 de 2014 *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*, o la ley que la modifique o reemplace, frente a la clasificación y reserva de la información, el Ministerio de Salud y Protección Social, deberá contar con la siguiente clasificación:

- Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal.
- Información Pública Clasificada: Es aquella información que, estando en poder o custodia de un sujeto obligado, pertenece al ámbito privado o semiprivado de una persona natural o jurídica. Su acceso podrá ser negado o exceptuado bajo circunstancias legítimas y necesarias, conforme a los derechos particulares consagrados en el artículo 18 de la Ley 1712 de 2014.
- Información Pública Reservada: Es aquella información que, estando en poder o custodia de un sujeto obligado, es exceptuada del acceso a la ciudadanía por daño a intereses públicos, cumpliendo con los requisitos establecidos en el artículo 19 de la Ley 1712 de 2014.

Cada activo y/o documento que haga parte del Sistema Integrado de Gestión (MIPG) debe poseer un etiquetado que identifique claramente el nivel de clasificación asignado. Además, el MSPS define los siguientes lineamientos:

1. Todos los equipos tecnológicos que forman parte del inventario del MSPS deben contar con un etiquetado y número único asignado para su fácil identificación y asignación.

2. Es responsabilidad de los funcionarios y contratistas velar por la custodia de los documentos e información confidencial, clasificada y/o reservada bajo su manejo. El manejo inadecuado generará acciones disciplinarias pertinentes a través de la Oficina de Control Interno Disciplinario.

3. Todos los aplicativos o sistemas de información del MSPS deben tener asignado un propietario responsable, quien definirá los niveles de privacidad de la información, así como los usuarios y permisos correspondientes.

4. Los funcionarios son responsables de actualizar y clasificar la información cuando esta requiera modificación. El dueño o responsable de la información tiene autonomía para reclasificarla cuando lo considere necesario, debiendo cambiar el rótulo o etiqueta y notificar a las partes pertinentes.

5. Los usuarios no deben usar indebidamente la información confidencial; está prohibido revelar, publicar o dar a conocer total o parcialmente a personas ajenas al MSPS, salvo a aquellos servidores públicos y contratistas que necesiten conocerla para cumplir con sus funciones.

6. Es responsabilidad de los encargados del manejo de la información asegurarse de que todos los datos y documentos estén claramente marcados y etiquetados para informar a todos los usuarios sobre su nivel de clasificación.

7. Se debe firmar un acuerdo de confidencialidad con terceras partes al requerir, entregar información electrónica, escrita, confidencial o interna, estableciendo restricciones sobre su uso.

8. Se deben implementar los mecanismos establecidos y apropiados de control de acceso a la información según su nivel de clasificación.

9. Los servidores públicos, contratistas y terceros no están autorizados para revelar información confidencial a terceros sin la aprobación del responsable o encargado de la información. La parte receptora debe firmar un acuerdo de confidencialidad respecto a la información recibida.

10. Es responsabilidad del encargado del proceso verificar que todos los activos de información estén debidamente etiquetados conforme a su clasificación.

10.6. POLÍTICA DE MANEJO DE MEDIOS

La presente política es aplicable a todos los servidores públicos, contratistas, terceros y partes interesadas que tengan algún vínculo con el Ministerio de Salud y Protección Social (MSPS), que por su rol y funciones propias de su cargo hagan uso de medios removibles dentro de la infraestructura del Ministerio.

En virtud de lo anterior, el MSPS establece los siguientes lineamientos de obligatorio cumplimiento:

1. Está restringido el uso y conexión no autorizada de cualquier elemento de almacenamiento extraíble para todos los servidores públicos, contratistas y terceros que desempeñen sus labores desde equipos de cómputo de la entidad.

2. Los medios de almacenamiento removibles, como cintas, discos duros removibles y dispositivos USB que contengan información institucional, deben ser controlados y protegidos físicamente.

3. La responsabilidad sobre la información contenida en los medios removibles recae en el servidor público, contratista o tercero a cargo del mismo, de acuerdo a la guía de custodia de medios.

4. El servidor público, contratista o tercero, es responsable de mantener asegurada la información, libre de software malicioso y cifrada si se considera confidencial, evitando poner en riesgo al MSPS.

5. Todos los usuarios deben velar por el buen uso de la información, su divulgación y distribución.

6. En caso de pérdida o robo de algún medio removible, debe ser reportado inmediatamente al responsable del proceso, informando sobre el nivel de importancia de la información.

7. Al término del vínculo laboral o contractual, los servidores públicos, contratistas y terceros deben devolver al responsable del proceso los medios removibles en los cuales gestionaron información institucional para proceder con el borrado seguro o disposición adecuada.

8. La reutilización, borrado y destrucción de medios removibles deberá realizarse bajo los lineamientos establecidos por el Grupo de Seguridad de la Información e Innovación, garantizando que la información borrada no pueda ser recuperada.

10.7. POLÍTICA DE CONTROL DE ACCESO

La presente política es aplicable a todos los servidores públicos, contratistas, terceros y partes interesadas que tengan algún vínculo con el Ministerio de Salud y Protección Social (MSPS), que por su rol y funciones propias de su cargo requieran acceso a los servicios y sistemas de información de la entidad.

Lineamientos para Áreas Seguras

1. Se consideran áreas seguras, los centros de cableado, el Circuito Cerrado de Televisión (CCTV), El Centro de Cómputo de MinSalud, Tesorería, Sala de Audiencias de Control Interno Disciplinario y el archivo central del MSPS.

2. El acceso físico y lógico al centro de cómputo y a las áreas de procesamiento de información será restringido y controlado por el Grupo de Soporte Informático, mediante mecanismos de seguridad establecidos.

3. Se deben garantizar las condiciones físicas y medioambientales necesarias para la protección y correcta operación de la infraestructura tecnológica del centro de datos.

Lineamientos para Acceso Lógico

4. El acceso a la información y a los sistemas de información debe estar restringido según los roles definidos por el MSPS, considerando la estricta necesidad de conocer y/o utilizar la información para el desarrollo de sus actividades.

5. El acceso a los activos de información del Ministerio debe estar restringido conforme a los niveles de clasificación establecidos, protegiendo la información contra accesos no autorizados. Se deben tener en cuenta los requisitos de seguridad de los sistemas de información y la autorización del acceso, basada en perfiles y roles definidos.

6. La autorización o rechazo para acceder a un sistema de información debe contar con la aprobación del jefe inmediato o supervisor del contrato, con la justificación necesaria, y, si es necesario, con la aprobación del responsable de la administración del sistema.

7. Todo acceso a una base de datos del MSPS debe ser controlado mediante un proceso de autenticación robusto.

8. Está prohibido que los servidores públicos, contratistas, terceros y partes interesadas accedan a los sistemas de información mediante el uso compartido de cuentas de usuario.

9. Se deben mantener actualizados los registros necesarios sobre las solicitudes, modificaciones y retiros de acceso para servidores públicos, contratistas y terceros, asegurando que estos registros puedan ser revisados periódicamente.

10. Todos los privilegios y derechos de uso de los sistemas de información deben suspenderse en el momento en que se evidencie mal uso de los roles o cuando se conozca la finalización del vínculo laboral. Por tal razón, cada encargado del área y/o dependencia debe notificar inmediatamente al Grupo de Soporte Informático para que se lleven a cabo las respectivas restricciones de acceso a la información.

Lineamientos para Acceso a Redes y Servicios de Red

11. El acceso a la red de datos del MSPS debe realizarse utilizando las credenciales de red de cada usuario.

12. Los servidores públicos, proveedores y terceros deben proteger y no compartir sus credenciales de acceso a la red y servicios de red que les son conferidos de acuerdo con su perfil.

13. Las contraseñas de usuarios privilegiados o superusuarios (administradores) de los servicios tecnológicos deben ser protegidas y almacenadas bajo la custodia del Líder del Proceso responsable del Sistema de Información, en coadministración con el Grupo de Soporte Informático.

14. Es responsabilidad de cada usuario realizar el cambio de su contraseña cuando sospeche que puede estar en conocimiento de terceras personas.

Lineamientos para Acceso Físico

1. Todos los servidores públicos, contratistas y terceros del Ministerio deben contar con un identificador único (ID del usuario, cuenta de usuario) para su uso personal, el cual es personal e intransferible.

10.8. POLÍTICA DE GESTIÓN DE CONTRASEÑAS

La presente política es aplicable a todos los funcionarios públicos, contratistas, terceros y partes interesadas que tengan algún vínculo con el Ministerio de Salud y Protección Social (MSPS), que por su rol y funciones propias del cargo requieran un usuario para el acceso a la infraestructura tecnológica y sistemas de información.

Los usuarios deben seguir las siguientes políticas para el uso y selección de las contraseñas de acceso, siendo responsables de cualquier acción realizada utilizando su cuenta de usuario y contraseña asignada:

1. Las contraseñas son de uso personal y no deben ser prestadas a otros usuarios bajo ninguna circunstancia.

2. Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

3. Las contraseñas deben establecerse de acuerdo con estándares y directrices mínimas para asegurar que no sean fáciles de descifrar. Se recomienda utilizar una combinación de caracteres alfanuméricos y símbolos especiales, mínimo debe contener 12 caracteres.

4. Las contraseñas no deben ser escritas en ningún medio, excepto cuando son entregadas en custodia conforme al procedimiento establecido.

5. Soporte Informático debe mantener deshabilitada la opción “recordar contraseña en este equipo” que ofrecen los programas o aplicaciones, en todos los equipos.

6. Se debe reportar cualquier sospecha de que otra persona esté utilizando su contraseña o usuario asignado, así como cualquier sospecha de uso indebido de una contraseña o usuario ajeno.

7. Las contraseñas deben cambiarse según los requerimientos establecidos por la infraestructura de procesamiento de información.

8. Los usuarios deben cambiar sus contraseñas la primera vez que utilicen las cuentas asignadas, siempre que el sistema lo permita.

9. El sistema de gestión de contraseñas bloqueará el acceso del usuario después de tres (3) intentos fallidos consecutivos de inicio de sesión.

10. El sistema bloqueará el equipo pasados dos minutos de inactividad.

11. Todos los usuarios y claves de acceso predeterminadas por el fabricante deben ser cambiadas inmediatamente después de la instalación y configuración del software o hardware (por ejemplo, appliances, impresoras, routers, herramientas de seguridad).

12. Los administradores de sistemas deben bloquear las claves de acceso cuando haya un cambio de proveedores o cuando un servidor público o contratista finalice su vínculo laboral o contractual con el MSPS.

10.9. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS Y GESTIÓN DE LLAVES

La presente política es aplicable a todos los servidores públicos, contratistas, terceros y partes interesadas que tengan algún vínculo con el Ministerio de Salud y Protección Social (MSPS) y que utilicen controles criptográficos y gestión de llaves según se requiera.

Esta política tiene como objetivo establecer directrices para la implementación y gestión de controles criptográficos con el fin de asegurar la confidencialidad, integridad y autenticidad de la información manejada por el Ministerio.

Lineamientos Generales

1. El MSPS implementa mecanismos de cifrado para proteger la confidencialidad e integridad de la información, basándose en un análisis de riesgo que identifica el nivel de protección necesario según la clasificación de la información.

2. El Grupo de Soporte Informático es responsable de utilizar herramientas de controles criptográficos para llevar a cabo el cifrado de los equipos utilizados por los servidores públicos, contratistas y terceros, cuando sea necesario.

3. Para las conexiones externas a la infraestructura tecnológica del MSPS, es responsabilidad de los grupos de, Grupo de Soporte Informático y Grupo de Sistemas de información e Infraestructura Tecnológica, garantizar que dichas conexiones cuenten con mecanismos seguros y cifrados.

4. En caso de solicitudes por parte de entes de control, organismos de seguridad del Estado u órdenes judiciales, la información cifrada podrá ser proporcionada en forma no cifrada previa autorización del propietario de la información y del Líder o responsable del Proceso.

5. Se deben mantener listados actualizados sobre las firmas digitales otorgadas y realizar seguimiento sobre las mismas. Los líderes de proceso son responsables de gestionar las llaves para firma electrónica (tokens), asignando una única llave por cada usuario que lo requiera según sus funciones.

6. Se debe controlar el ciclo de vida completo de las llaves criptográficas, incluyendo su generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción.

7. Se deben implementar controles criptográficos para:
   - La protección de claves de acceso a sistemas, datos y servicios.
   - La transmisión segura de información clasificada.
   - El almacenamiento seguro en unidades compartidas.
   - La protección durante el almacenamiento y transmisión en dispositivos móviles, correos electrónicos y servicios en la nube (incluyendo discos duros externos, dispositivos USB, teléfonos celulares, OneDrive, SFTP).

8. El grupo Soporte Informático es responsable de garantizar que la información esté debidamente cifrada utilizando las herramientas proporcionadas por el Ministerio, independientemente del medio donde se almacene (computadores portátiles, discos duros extraíbles, dispositivos móviles, etc.).

9. Los servidores públicos, contratistas y terceros son responsables por custodiar y proteger las firmas digitales y llaves asignadas.

10. Las firmas digitales y llaves asignadas deben utilizarse únicamente para cumplir con las funciones asignadas por el MSPS.

11. Los usuarios deben abstenerse de publicar, prestar o ceder sus llaves asignadas y tomar las medidas necesarias para evitar su uso no autorizado.

12. Es responsabilidad del personal informar oportunamente al Líder del Proceso y al Grupo de Seguridad de la Información sobre cualquier irregularidad relacionada con el servicio de firma digital.

13. En caso de evidenciar falsedad en los datos suministrados por el solicitante, se procederá a suspender el servicio relacionado con firmas digitales y llaves criptográficas.

14. El MSPS establece que las firmas electrónicas se utilizarán exclusivamente para gestionar documentos hacia entidades externas o para firmar documentos internos considerados masivos.

15. El MSPS garantizará que las llaves para firma electrónica sean entregadas mediante un ente acreditado dentro del país.

16. Para aquellos servidores públicos, contratistas o terceros que requieran el uso del servicio de firma electrónica por su rol funcional, el Líder del Proceso evaluará la solicitud y decidirá sobre su asignación o rechazo basándose en justificaciones presentadas en el memorando correspondiente.

17. Es responsabilidad del personal solicitar la renovación o cancelación del servicio de firma electrónica según corresponda (finalización del contrato, cambio de funciones, finalización del vínculo laboral, fecha de caducidad entre otros).

10.10. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

La presente política es aplicable a todos los servidores públicos, contratistas, terceros y partes interesadas que tengan algún vínculo con el Ministerio de Salud y Protección Social (MSPS), que utilicen estaciones de trabajo, PCs y equipos portátiles asignados para el cumplimiento de sus funciones. Su objetivo es establecer lineamientos que garanticen la protección de la información y los datos, minimizando el riesgo de accesos no autorizados, pérdida o daño de la información.

Lineamientos Generales

1. El usuario debe bloquear el equipo asignado cada vez que se retire de su puesto físico de trabajo, independientemente de la razón de la ausencia, con el fin de garantizar la protección de la información y prevenir accesos no autorizados.

2. Es deber de los usuarios mantener su escritorio físico y virtual libre de información clasificada que pueda ser visualizada, copiada o utilizada por personal no autorizado. No se permite abandonar el puesto de trabajo al finalizar la jornada laboral dejando documentos físicos en el escritorio, almacenando información en gavetas sin llave, o dejando equipos encendidos.

3. Con el fin de promover la política de cero papel, se debe evitar imprimir documentos a menos que sea estrictamente necesario. Los documentos impresos que contengan información reservada o pública clasificada no deben dejarse en las impresoras y deben ser retirados de inmediato para prevenir divulgaciones no autorizadas.

4. Si un documento confidencial que contengan información reservada, o pública clasificada, ha sido impreso y no se va a utilizar para ningún trámite o archivo, no debe ser reutilizado ni reciclado. En estos casos, es obligatorio destruir el papel que contenga dicha información antes de desecharlo en el reciclaje, asegurando así la protección de la información sensible.

5. La información confidencial (documentos físicos o unidades de almacenamiento externo) debe ser protegida bajo llave durante el horario no hábil o cuando los puestos de trabajo estén desatendidos.

6. Los archivos que contengan información sensible o confidencial deben almacenarse en rutas que impidan el acceso fácil por parte de terceros no autorizados, evitando su ubicación en el área del escritorio virtual del equipo. Se prohíbe el escritorio de pantalla para tal fin

7. El Grupo de Soporte Informático establecerá controles automáticos para bloquear las sesiones de los usuarios tras dos minutos de inactividad.

8. Al finalizar la jornada laboral, los usuarios deben cerrar todas las aplicaciones y dejar los equipos apagados (se pueden exceptuar los que estén debidamente autorizados, para quedar en hibernación). El Grupo de Soporte

Informático garantizará que todas las estaciones de trabajo estén debidamente aseguradas mediante mecanismos de seguridad apropiados.

9. Los servidores públicos, contratistas y terceros que atiendan al público deben almacenar documentos y dispositivos de almacenamiento bajo llave, ubicando el equipo de cómputo en un lugar que evite el acceso o revisión por parte de visitantes no autorizados.

10. El Grupo de Soporte Informático configurará todos los equipos en los dominios del Ministerio para ocultar automáticamente los íconos, accesos directos o documentos que se encuentren en el escritorio cuando no estén en uso.

10.11. POLÍTICA DE GESTIÓN DE REDES

El Ministerio de Salud y Protección Social (MSPS) garantiza la seguridad de la información que se transporta a través de las redes de comunicación e instalaciones de procesamiento de información. Por lo tanto, todos los servidores públicos, contratistas, terceros y partes interesadas que generen y/o envíen información por los canales autorizados por el Ministerio deben cumplir obligatoriamente con los siguientes lineamientos:

1. El Grupo de Soporte Informático es responsable de controlar los accesos a los servicios internos y externos conectados a toda la red del Ministerio.

2. Se deben implementar mecanismos de control de acceso mediante la segmentación de las redes, en función de los grupos de servicios como usuarios, sistemas de información y componentes físicos y lógicos.

3. Los servidores públicos, contratistas, terceros y partes interesadas deben utilizar la red corporativa de Internet exclusivamente para el desarrollo de actividades relacionadas con sus funciones en el Ministerio.

4. No se permite que los servidores públicos, contratistas, terceros y partes interesadas conecten elementos de red (como switches, enrutadores, módems, etc.) a las estaciones de trabajo o puntos de acceso del Ministerio sin la autorización del Grupo de Soporte Informático y del Grupo de Seguridad de la Información y Protección de Datos Personales.

5. El MSPS debe cifrar la información durante su transporte y almacenamiento utilizando herramientas tecnológicas adecuadas, como firewalls, VPNs, certificados SSL y canales cifrados.

6. Las redes de comunicación del Ministerio deben contar con registros o logs de auditoría que permitan realizar un seguimiento detallado de las operaciones realizadas sobre las mismas. Asimismo, deben disponer de sistemas de monitoreo para gestionar adecuadamente su comportamiento.

7. El MSPS podrá implementar redes de comunicación en ambientes físicos, virtuales o en la nube, ya sean propias o con terceros, aplicando los controles de seguridad pertinentes según el contexto.

8. Es responsabilidad del Grupo de Soporte Informático e Infraestructura de TI garantizar que los desarrolladores internos o externos tengan acceso limitado y controlado a los datos y archivos presentes en los ambientes de producción, preproducción y desarrollo.

10.12. POLÍTICA DE COPIAS DE SEGURIDAD

La presente política es aplicable a los sistemas de información y repositorios de almacenamiento de información de trabajo de los servidores públicos, contratistas, terceros y partes interesadas que tengan algún vínculo con el Ministerio de Salud y Protección Social (MSPS).

La gestión de copias de respaldo de información debe garantizar la confidencialidad, integridad y disponibilidad de la información y los datos personales.

Lineamientos Generales

1. Los Grupos de Soporte Informático e Infraestructura de Tecnología de la Información deberán realizar copias de respaldo periódicas sobre la configuración e información contenida en la infraestructura tecnológica del MSPS.

2. Es responsabilidad de los propietarios de los sistemas de información y del Grupo de Soporte Informático determinar la periodicidad y el tipo de copia de respaldo necesaria para la configuración e información en la infraestructura tecnológica.

3. Los Grupos de Soporte Informático e Infraestructura de TI deberán llevar a cabo las restauraciones necesarias cuando se requieran las copias de respaldo para garantizar el correcto funcionamiento de la infraestructura física.

4. Cada servidor público, contratista y tercero es responsable de realizar las copias de seguridad de la información en las rutas del repositorio establecidas por el Grupo de Soporte Informático, asegurando así la confidencialidad, integridad y disponibilidad.

5. El repositorio compartido debe utilizarse exclusivamente para información transitoria. En caso de requerir una copia de la información almacenada en este servicio, se deberá solicitar formalmente al Grupo de Soporte Informático, garantizando así la gestión adecuada y segura de los datos.

6. Se debe utilizar el recurso OneDrive a través de Office 365 en las cuentas asignadas a cada usuario para el almacenamiento y compartición de información del Ministerio, asegurando que toda la información cumpla con las políticas de seguridad y acceso establecidas. El administrador de Office 365, en conjunto con Gestión Documental, son los encargados de capacitar en el uso de esta herramienta, para el almacenamiento de información teniendo en cuenta la normativa de archivo.

7. En caso de requerir un respaldo periódico, la información debe ser almacenada en la carpeta designada "MSPS", ubicada en la ruta de acceso "Documentos" de cada equipo. Este procedimiento asegura la organización y disponibilidad adecuada de los datos respaldados.

8. Los servidores públicos, contratistas y terceros deben realizar la depuración regular de la información para optimizar los recursos asignados por el Ministerio.

9. Los tiempos de preservación para las copias de seguridad deben definirse teniendo en cuenta los lineamientos establecidos por los propietarios de los sistemas y el Grupo de Soporte Informático. Este grupo también deberá asegurar que las restauraciones se realicen conforme a los cambios o actualizaciones tecnológicas pertinentes.

10. Para ejecutar copias adicionales o nuevas, el responsable debe formular un requerimiento al Grupo de Soporte Informático o Infraestructura de TI, especificando la necesidad del respaldo, tipo de información a salvaguardar, frecuencia requerida, niveles de clasificación y tiempo de retención.

11. Se deben documentar todas las actividades relacionadas con el tratamiento y gestión de las copias de seguridad para asegurar su trazabilidad.

12. Al finalizar el ciclo útil del medio utilizado para las copias de seguridad, este debe ser eliminado o dispuesto adecuadamente para evitar la recuperación no autorizada de la información almacenada

10.13. POLÍTICA DE RELACIÓN CON PROVEEDORES

La presente política es aplicable a terceros, proveedores y partes interesadas que tengan algún vínculo con el Ministerio de Salud y Protección Social (MSPS) y que requieran acceso a los activos de información del Ministerio, de acuerdo con los niveles acordados de seguridad digital y prestación de servicios.

El objetivo de esta política es establecer lineamientos claros para la gestión de relaciones con proveedores, garantizando la protección de la información y el cumplimiento de las políticas de seguridad del Ministerio.

Lineamientos Generales

1. Los servidores públicos y contratistas autorizados por los Líderes de Proceso deberán proporcionar acceso a la información del MSPS a los proveedores únicamente cuando sea necesario para el cumplimiento del objeto contractual, aplicando el principio de mínimos privilegios.

2. El Líder de Proceso es responsable de socializar las políticas de seguridad de la información del Ministerio con todos los proveedores con los que se tenga un vínculo contractual, asegurando su comprensión y cumplimiento.

3. Se deben establecer y monitorear las condiciones para la comunicación y transmisión segura de información desde el inicio del contrato entre el Ministerio y los proveedores de servicios.

4. Los proveedores deben ser notificados que todos los cambios en los servicios tecnológicos contratados deben ser comunicados a los supervisores de contrato con anticipación. Estos cambios serán analizados por el Grupo de Seguridad de la Información y Protección de Datos Personales para su aprobación.

5. Todos los proveedores que tengan un vínculo contractual con el Ministerio que implique intercambio, uso o procesamiento de información deberán firmar acuerdos de confidencialidad y no divulgación, asegurando así la protección de la información sensible.

6. Todos los incidentes de seguridad relacionados con la ejecución del contrato deben ser reportados inmediatamente por los supervisores de contrato o sus delegados, quienes también deberán presentar un plan de mitigación y solución.

7. Es responsabilidad de los supervisores de contrato realizar un seguimiento continuo a los proveedores y terceros con los que el Ministerio tenga relaciones contractuales, asegurando el cumplimiento normativo.

8. Los supervisores deben verificar el cumplimiento de los controles relacionados con el software base instalado y licenciamiento, así como hacer extensivos estos controles a equipos informáticos proporcionados por terceros cuando sea necesario.

9. Los supervisores son responsables de requerir a los proveedores que mantengan una capacidad adecuada para prestar servicios, junto con planes ejecutables que aseguren la continuidad del servicio acordada al inicio del contrato, especialmente después de fallas significativas o desastres.

10. Los supervisores evaluarán continuamente el desempeño y cumplimiento normativo por parte de los proveedores, promoviendo mejoras en la relación contractual y en la calidad del servicio prestado, en beneficio del MSPS.

10.14. POLÍTICA DE DESARROLLO SEGURO

La presente política es aplicable a todos los desarrollos de aplicaciones o despliegues dentro de la infraestructura del Ministerio de Salud y Protección Social (MSPS), realizados a través de servidores públicos, contratistas y acuerdos con proveedores.

El objetivo de esta política es establecer lineamientos que aseguren un desarrollo seguro de software, garantizando la protección de la información y el cumplimiento de las normativas de seguridad.

Lineamientos Generales

1. El Grupo de Sistemas de Información y Datos debe establecer una metodología de desarrollo seguro de software que se ajuste a las necesidades específicas del Ministerio.

2. Todos los proyectos de desarrollo y adquisición de sistemas, ya sean propios o de terceros, deben incluir requisitos de seguridad de la información desde la etapa de diseño, aplicables a lo largo del ciclo de vida del sistema.

3. Se deben habilitar registros o logs de auditoría sobre el desarrollo del software para asegurar un seguimiento detallado desde el inicio del proceso.

4. Todo proyecto relacionado con la implementación de nuevos sistemas o aplicaciones debe ser coordinado con el Grupo de Sistemas de Información y Datos con suficiente antelación para garantizar la disponibilidad de los recursos tecnológicos necesarios.

5. El Grupo de Sistemas de Información y Datos debe aplicar mecanismos adecuados para proteger la información transaccional en las aplicaciones, evitando alteraciones o pérdidas durante el desarrollo.

6. Es responsabilidad del Grupo de Sistemas de Información y Datos contar con sistemas para el control de versiones que administren los cambios en los sistemas desarrollados o desplegados dentro del MSPS.

7. El Grupo debe verificar que las aplicaciones que manejan transacciones adquiridas o desarrolladas por terceros cumplan con requisitos mínimos de seguridad, tales como:

    - Acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

- Uso de firmas electrónicas para las partes que hacen la transacción.
- Sistemas de autenticación con usuario y contraseña.
- Cifrado de la información, de la transacción y del canal utilizado.
- El Cifrado debe estar dado por una entidad certificadora.
- Registros o logs de auditoría sobre la transacción.
- Los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no deben ser accesibles desde los ambientes de producción cuando no se requiera.
- Desarrollar las aplicaciones de tal forma que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Suministrar opciones de desconexión o cierre de sesión de las aplicaciones (logout) que permitan terminar completamente con la sesión o conexión asociada.
- Asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Asegurar el manejo de operaciones sensibles o críticas en las aplicaciones desarrolladas permitiendo el uso de parámetros adicionales de verificación.
- Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- No incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes.
- Certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- Asegurar que no se permite que las aplicaciones desarrolladas ejecuten comandos directamente en el sistema operativo.

8. El Grupo de Sistemas de Información e Infraestructura Tecnológica debe generar metodologías para realizar pruebas al software desarrollado, incluyendo pautas para seleccionar escenarios, niveles, tipos y datos necesarios para pruebas. Todas estas actividades deben estar documentadas.

9. Todo desarrollo o despliegue dentro del MSPS debe cumplir con los requisitos establecidos sobre seguridad de la información y privacidad de datos personales.

10. Se deben establecer repositorios seguros para el software, protegidos mediante controles adecuados como cifrado e identificación por usuario y contraseña.

11. Debe existir un control riguroso del versionamiento del software desarrollado.

12. Los controles necesarios deben ser validados para asegurar que las migraciones entre ambientes (desarrollo, preproducción y producción) han sido aprobadas siguiendo los procedimientos establecidos.

13. Todo desarrollo o despliegue debe someterse a una revisión técnica que incluya aspectos funcionales, técnicos y consideraciones sobre seguridad antes de su implementación en producción.

14. Los supervisores de contrato deben incluir cláusulas legales, técnicas, operativas y relacionadas con seguridad en todos los contratos, acuerdos o convenios que aseguren un desarrollo seguro para el Ministerio.

10.15. POLÍTICA DE TRANSFERENCIA DE LA INFORMACIÓN

La presente política es aplicable a servidores públicos, contratistas, terceros y partes interesadas que, por sus funciones, transfieran o transmitan información con entidades externas. Su objetivo es establecer lineamientos claros para la transferencia de información, garantizando la protección de la confidencialidad, integridad y disponibilidad de los datos.

Lineamientos Generales

1. El Ministerio de Salud y Protección Social (MSPS) debe proteger la información durante su intercambio, tanto a nivel interno como externo, para preservar su confidencialidad, integridad y disponibilidad.

2. Los servidores públicos, contratistas y terceros autorizados que requieran transferir información del Ministerio no deben utilizar herramientas personales o no autorizadas para el intercambio de información.
3. El Grupo de Soporte Informático es responsable de implementar, gestionar y mantener los controles de seguridad necesarios para proteger la información que se transfiere a entidades externas y viceversa.

4. Los servidores públicos, contratistas y terceros autorizados no deben enviar copias, divulgar o emplear indebidamente datos e información contenida en las aplicaciones, bases de datos y sistemas del Ministerio para fines distintos al cumplimiento de sus obligaciones contractuales.

5. Las herramientas y medios utilizados para la transferencia de información hacia entidades externas deben incorporar controles criptográficos para proteger la confidencialidad, integridad y autenticidad de los datos transmitidos.

6. Los servidores públicos, contratistas y terceros autorizados son responsables de no comprometer a la Entidad por difamación, acoso o suplantación mediante la transferencia de información con fines personales o no autorizados.

7. Todos los intercambios de información deben estar respaldados por contratos, convenios o acuerdos formalizados ante el Ministerio, que establezcan los medios, controles en el tratamiento de la información, cláusulas de confidencialidad y otros lineamientos establecidos por la Entidad.

8. Los servidores públicos, contratistas y terceros autorizados deben firmar acuerdos de confidencialidad y privacidad cuando sea necesario para proteger la información sensible.

9. Es responsabilidad y obligación de los servidores públicos, contratistas y terceros autorizados mantener una custodia adecuada de la información mientras esta se encuentra en tránsito.

10.16. POLÍTICA DE INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS

La presente política es aplicable a todos los servidores públicos, contratistas, terceros y partes interesadas que, por sus funciones, requieran llevar a cabo la instalación de software dentro de los sistemas operativos del Ministerio de Salud y Protección Social (MSPS). Su objetivo es establecer lineamientos claros para la instalación de software, garantizando la seguridad de la infraestructura tecnológica del Ministerio.

Lineamientos Generales

1. El Grupo de Soporte Informático es el único autorizado para realizar la instalación y desinstalación de software en los sistemas operativos de los equipos de cómputo e infraestructura tecnológica del MSPS.

2. Todos los equipos de cómputo del Ministerio deben ser entregados a los usuarios con privilegios estándar, evitando privilegios de administración para prevenir modificaciones no autorizadas.

3. Los usuarios que requieran la instalación de software para cumplir con sus funciones deben presentar una solicitud formal al Grupo de Soporte Informático, quien evaluará la justificación y disponibilidad del licenciamiento necesario.

4. El Grupo de Soporte Informático debe asegurarse de que todo software o sistema operativo instalado en la infraestructura tecnológica del Ministerio cuente con el respectivo licenciamiento, con el fin de prevenir repercusiones legales y daños técnicos en los equipos.

5. El Grupo de Soporte Informático debe validar los riesgos asociados a la migración hacia nuevas versiones del software operativo cuando sea requerido por el Ministerio, asegurando que el funcionamiento de los sistemas de información y herramientas se mantenga intacto tras las actualizaciones.

6. Antes de proceder con cualquier instalación o actualización, se deben realizar pruebas adecuadas para verificar la compatibilidad y el correcto funcionamiento del software con las aplicaciones existentes.

7. Todas las instalaciones y desinstalaciones deben ser documentadas adecuadamente, manteniendo un registro actualizado que permita auditorías futuras y trazabilidad en la gestión del software.

10.17. POLÍTICA DE TRABAJO REMOTO

La presente política es aplicable a todos los servidores públicos, contratistas, terceros y partes interesadas que tengan algún vínculo con el Ministerio de Salud y Protección Social (MSPS) y que, por sus funciones, requieran acceder a la infraestructura tecnológica del Ministerio de forma remota. Su objetivo es establecer lineamientos claros para el trabajo remoto, garantizando la seguridad de la información y el cumplimiento de las normativas vigentes.

Lineamientos Generales

1. El trabajo remoto se regirá por lo establecido en el Decreto 555 de 2022, que regula las condiciones del trabajo remoto en Colombia, así como por cualquier normativa que lo modifique o complemente.

2. El Ministerio debe proporcionar métodos seguros para realizar el trabajo remoto, utilizando conexiones como VPN (Red Privada Virtual), VDI (Infraestructura de Escritorios Virtuales) y FTP (Protocolo de Transferencia de Archivos), entre otros.

3. Es responsabilidad de los servidores públicos, contratistas y terceros aplicar los lineamientos de seguridad y privacidad de la información al desarrollar sus actividades laborales o contractuales fuera de las instalaciones del Ministerio.

4. El Grupo de Soporte Informático debe verificar que se cumplan los controles de seguridad establecidos para el trabajo remoto en la infraestructura del Ministerio.

5. Las conexiones remotas a los recursos tecnológicos del Ministerio deben restringirse únicamente a equipos autorizados.

6. El Grupo de Soporte Informático debe monitorear el uso de los recursos e infraestructura dispuestos para el trabajo remoto, previniendo y detectando vulnerabilidades, ataques cibernéticos y otros incidentes de seguridad.

7. Los servidores públicos, contratistas y terceros deben asegurarse de que los equipos utilizados para el trabajo remoto estén configurados con medios adecuados de autenticación, como contraseñas, PINs o huellas dactilares. Además, deberá tener en cuenta:

    - Cada funcionario debe tener una sesión exclusiva para el Ministerio en su equipo personal o de trabajo, asegurando que el acceso a la infraestructura tecnológica del Ministerio esté restringido y controlado.
    - Se debe implementar un sistema de doble factor de autenticación (2FA) para acceder a los recursos del Ministerio. Teniendo en cuenta los parámetros de combinación de una contraseña con un código enviado a un dispositivo móvil o un token de seguridad, garantizando así una capa adicional de protección.
    - Los servidores públicos, contratistas y terceros son responsables legalmente por el manejo adecuado de la información a la que acceden durante su trabajo remoto, esto incluye:
        - Descargar información desde la nube, editarla y cargarla nuevamente en los sistemas del Ministerio.
        - Asegurarse de que toda información tratada cumpla con las políticas de seguridad y privacidad establecidas por el Ministerio.
        - Proteger la información clasificada y sensible, evitando su divulgación no autorizada.
    - Los usuarios deben ser conscientes de su responsabilidad en la protección de la información y deben recibir capacitación sobre las mejores prácticas en seguridad informática y manejo seguro de datos.

8. La información tratada durante el trabajo remoto debe ser almacenada en los servicios o medios proporcionados por el Ministerio, asegurando su protección y compartición adecuada. Además, deben resguardar la información según la clasificación establecida para los activos del Ministerio.

9. Es responsabilidad de los servidores públicos, contratistas y terceros informar inmediatamente al Grupo de Seguridad de la Información y Protección de Datos Personales sobre cualquier evento que comprometa la seguridad en los equipos utilizados para el trabajo remoto.

10. Los usuarios deben utilizar únicamente las aplicaciones colaborativas y plataformas de teleconferencia autorizadas por el Ministerio, cumpliendo con sus condiciones de uso. Está prohibido acceder a programas no controlados o no autorizados.

11. Al utilizar equipos personales para realizar trabajo remoto, se deben cumplir como mínimo las siguientes condiciones:

    - Mantener actualizado el sistema operativo.
    - Garantizar el buen funcionamiento del equipo.
    - Contar con un antivirus instalado, activo y actualizado; así como con licenciamiento adecuado del software utilizado.

12. Se debe garantizar el derecho a la desconexión laboral para todos los trabajadores remotos, conforme a lo establecido en la normativa vigente.

10.18. POLÍTICA DE SEGURIDAD EN LA NUBE

La presente política es aplicable a todos los servidores públicos, contratistas, terceros y partes interesadas que utilicen servicios en la nube para almacenar, procesar o transmitir información del Ministerio de Salud y Protección Social (MSPS). Su objetivo es establecer lineamientos claros para el uso seguro de servicios en la nube, garantizando la protección de la información y el cumplimiento de las normativas vigentes.

Lineamientos Generales

1. Los servicios en la nube deben ser proporcionados por proveedores que cumplan con estándares de seguridad reconocidos y que demuestren cumplimiento con las normativas colombianas sobre protección de datos personales.

2. Antes de implementar servicios en la nube, se debe realizar una evaluación de riesgos para identificar posibles amenazas y vulnerabilidades asociadas al uso de estos servicios.

3. La información sensible que se almacene o transmita a través de servicios en la nube debe ser cifrada tanto en reposo como en tránsito, utilizando protocolos seguros.

4. Se deben establecer controles de acceso estrictos para garantizar que solo el personal autorizado tenga acceso a la información almacenada en la nube.

5. Todos los contratos con proveedores de servicios en la nube deben incluir cláusulas específicas sobre la seguridad de la información, incluyendo responsabilidades en caso de brechas de seguridad y manejo adecuado de datos personales.

6. Se debe implementar un sistema de monitoreo continuo para detectar actividades inusuales o no autorizadas en los servicios en la nube. Se deben realizar auditorías periódicas para asegurar el cumplimiento con las políticas establecidas.

7. Debe existir un plan documentado para responder a incidentes relacionados con la seguridad en la nube, incluyendo procedimientos para notificar a las partes afectadas y a las autoridades competentes cuando sea necesario.

8. Se promoverán programas de capacitación continuos sobre el uso seguro de servicios en la nube para todos los usuarios involucrados, asegurando que comprendan los riesgos y las mejores prácticas.

10.19. POLÍTICA DE USO ACEPTABLE DEL CORREO ELECTRÓNICO

La presente política es aplicable a todos los servidores públicos, contratistas, terceros y partes interesadas que utilicen el correo electrónico institucional del Ministerio de Salud y Protección Social (MSPS). Su objetivo es establecer directrices claras sobre el uso adecuado del correo electrónico institucional.

Lineamientos Generales

1. El correo electrónico institucional debe ser utilizado exclusivamente para actividades relacionadas con las funciones laborales y contractuales dentro del Ministerio.

2. Los usuarios deben evitar enviar información sensible o clasificada a través del correo electrónico sin las medidas adecuadas de cifrado y autorización previa.

3. Está prohibido utilizar el correo electrónico institucional para enviar o recibir material pornográfico, ofensivo o no relacionado con las actividades laborales.

4. Los usuarios deben tener cuidado al abrir archivos adjuntos provenientes de fuentes desconocidas o no verificadas, ya que pueden contener malware o virus informáticos. Todos los funcionarios deben estar capacitados en la identificación o sospecha de correos maliciosos.

5. No se debe utilizar el correo electrónico institucional para fines personales, incluyendo el registro en sitios web no relacionados con las funciones del Ministerio.

6. El envío de correos masivos debe ser autorizado previamente por un superior y cumplir con las políticas establecidas sobre comunicación interna.

7. Cualquier incidente relacionado con el uso del correo electrónico debe ser reportado inmediatamente al Grupo de Seguridad de la Información y Protección de Datos Personales.

8. Se promoverán programas continuos sobre el uso seguro del correo electrónico para todos los usuarios involucrados, asegurando que comprendan los riesgos asociados y las mejores prácticas.

10.20. POLÍTICA DE USO E IMPLEMENTACIÓN DE INTELIGENCIA ARTIFICIAL

Política para el Aseguramiento de la Información y Datos Personales en la Implementación de Soluciones de Inteligencia Artificial[22]

[22] Fuentes:
- Convenio Marco sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho del Consejo de Europa.
- Manual de Políticas de Seguridad de la Información del Ministerio de Salud y Protección Social.
- Normativas nacionales e internacionales en materia de protección de datos y ciberseguridad.
- CONPES 4144 de 2025
- Recomendación sobre la ética de Inteligencia Artifical de la UNESCO (2024)
- Circular externa 02 de 2024

1. Propósito y Aplicación

Esta política tiene como finalidad establecer los lineamientos para el uso, desarrollo e implementación de sistemas de Inteligencia Artificial (IA) en el Ministerio de Salud y Protección Social, asegurando el cumplimiento de la normativa vigente, especialmente en lo relacionado con la protección de datos personales. Aplica a todas las dependencias del Ministerio que desarrollen, implementen o utilicen soluciones de IA, así como a los proveedores externos que suministren tales soluciones.

2. Principios Rectores

El uso de la IA debe basarse en los siguientes principios rectores:

- Respeto a los Derechos Humanos: Los sistemas de IA deben diseñarse y operar de forma que respeten la dignidad humana, la privacidad y los derechos fundamentales de todas las personas.
- Seguridad y Protección: Se deben implementar medidas para asegurar la integridad, disponibilidad y confidencialidad de los datos procesados por sistemas de IA, protegiendo contra accesos no autorizados y ciberataques.
- Proporcionalidad e Inocuidad: El uso de sistemas de IA debe limitarse a lo necesario para cumplir con objetivos legítimos, evaluando riesgos para prevenir daños derivados de usos ilegítimos.
- Derecho a la Intimidad y Protección de los Datos: Debe garantizarse la protección de la privacidad durante todo el ciclo de vida de la IA, con marcos adecuados para la protección de datos.
- Responsabilidad y Rendición de Cuentas: Los sistemas de IA deben ser auditables y trazables, con mecanismos de supervisión y evaluación de impacto para prevenir conflictos con los derechos humanos y posibles riesgos medioambientales.
- Transparencia y Explicabilidad: El despliegue ético de los sistemas de IA depende de su transparencia y explicabilidad (T&E). El nivel de T&E debe ser adecuado al contexto, ya que puede haber tensiones entre T&E y otros principios como la privacidad, la seguridad y la protección.
- Supervisión y Decisión Humanas: Siempre debe ser posible atribuir la responsabilidad ética y jurídica a personas físicas o entidades jurídicas en el uso de sistemas automatizados.
- Equidad y No Discriminación: Los actores de la IA deben promover la justicia social, garantizando que sus beneficios sean accesibles para todos y previniendo discriminación. Adoptando un enfoque inclusivo para garantizar que los beneficios de la IA sean accesibles para todos.
- Sostenibilidad: La IA debe evaluarse en términos de sostenibilidad, alineándose con los Objetivos de Desarrollo Sostenible (ODS) de la ONU.

3. Lineamientos para el Uso de Plataformas de IA en Línea

- Evaluación de Riesgos: Antes de utilizar plataformas de IA en línea (ChatGPT, Gemini, Claude, DeepSeek, etc.), se realizará una evaluación exhaustiva de riesgos para identificar impactos en la privacidad y seguridad de la información sensible a través de metodologías tales como PIA-Evaluación de impacto a la privacidad.
- Protección de Datos Personales: Los datos personales que se compartan con plataformas de IA en línea deben cumplir con la normativa de protección de datos vigente, garantizando el consentimiento informado de los titulares de los datos. Para el efecto se deberá efectuar la debida clasificación de los datos personales a compartir en las plataformas de IA.
- Confidencialidad de Información Sensible: La información representada en datos que ostenten la clasificación de "sensibles" según la Ley, no podrán compartirse o procesarse en plataformas de IA en línea que no ofrezcan garantías adecuadas de seguridad y confidencialidad.
- Uso Ético y Responsable: Los funcionarios deben usar las plataformas de IA de manera ética y responsable, verificando las respuestas generadas por estas plataformas antes de tomar decisiones críticas.

4. Desarrollo y Adquisición de Sistemas de IA

- Cumplimiento Normativo: Todo desarrollo o adquisición de sistemas de IA debe cumplir con las leyes y regulaciones aplicables sobre derechos humanos, protección de datos y seguridad de la información.
- Evaluación de Impacto: Se realizará una evaluación de impacto en derechos fundamentales antes de la implementación de cualquier sistema de IA, identificando y mitigando riesgos.
- Selección de Proveedores: Los proveedores de soluciones de IA deben demostrar compromiso con prácticas éticas, transparencia en los algoritmos y cumplimiento de estándares de seguridad y privacidad.

5. Capacitación y Sensibilización

El Ministerio proporcionará programas de capacitación continua a sus funcionarios sobre el uso ético y seguro de la IA, incluyendo la identificación y mitigación de sesgos, protección de datos y supervisión de sistemas automatizados.

6. Cumplimiento de la Política

Se establecerán mecanismos de monitoreo para asegurar que tanto las iniciativas internas como aquellas contratadas a través de terceros cumplan con los lineamientos de esta política.

7. Actualización de la Política

Esta política será revisada y actualizada regularmente para ajustarse a los avances tecnológicos, cambios normativos y mejores prácticas internacionales en el ámbito de la inteligencia artificial.

8. Responsabilidades

- Funcionarios del Ministerio: Deben adherirse a los lineamientos de esta política y reportar cualquier incidente o vulnerabilidad relacionada con el uso de sistemas de IA.
- Grupo de Seguridad de la Información e Innovación: Es el encargado de coordinar la implementación de esta política, supervisar su cumplimiento y ofrecer orientación sobre el uso seguro y ético de la IA.
- Proveedores Externos: Los proveedores deben garantizar que sus soluciones de IA cumplan con los estándares de seguridad, privacidad y ética establecidos por el Ministerio.

Implementación

La implementación de esta política reafirma el compromiso del Ministerio de Salud y Protección Social con el uso responsable de la inteligencia artificial, asegurando que sus beneficios se alcancen sin comprometer los derechos y la seguridad de los ciudadanos.

11. ACCIONES DISCIPLINARIAS PARA LAS VIOLACIONES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Ministerio de Salud y Protección Social (MSPS) publicará en la Intranet un manual que contiene las políticas de seguridad de la información, disponible para todos los servidores que utilicen los servicios de tecnologías de la información y los activos de información de la Entidad. Se espera el cumplimiento estricto de lo allí establecido.

Desconocimiento y Responsabilidad

El desconocimiento de la política de seguridad de la información por parte de funcionarios, contratistas y terceros puede dar lugar a acciones disciplinarias. El Ministerio llevará a cabo los procesos disciplinarios pertinentes a través de la Oficina de Control Interno Disciplinario. Las siguientes actuaciones constituyen violaciones a la seguridad de la información y pueden resultar en sanciones:

1. No informar sobre incidentes de seguridad o violaciones a las políticas cuando se tenga conocimiento.
2. No mantener actualizada la información sobre los activos a su cargo.
3. No proteger adecuadamente la información cuando se ausente del puesto o al finalizar la jornada laboral, incluyendo documentos impresos con información reservada o clasificada.
4. No almacenar información digital del Ministerio en los lugares designados, dejando datos sensibles en carpetas compartidas o ubicaciones no seguras.
5. Solicitar el cambio de contraseña o desbloqueo de equipo de otro usuario.
6. Utilizar la red del Ministerio para obtener, mantener o difundir material pornográfico, ofensivo, cadenas no autorizadas o correos masivos.

7. Instalar o utilizar software no relacionado con las actividades laborales que degrade el desempeño de la infraestructura tecnológica del Ministerio.

8. Enviar información del Ministerio a través de correos electrónicos personales sin autorización.

9. Conectar dispositivos de almacenamiento externo a los equipos sin autorización previa.

10. Permitir el acceso a la red institucional sin autorización previa.

11. Mostrar negligencia en el cuidado de equipos, dispositivos portátiles o móviles entregados para actividades del Ministerio.

12. No cumplir con las actividades designadas para proteger los activos de información del Ministerio.

13. Descuidar documentación crítica, reservada o clasificada sin las medidas adecuadas para su protección.

14. Almacenar información crítica en dispositivos que no pertenezcan al Ministerio o conectar equipos personales a la red sin autorización.

15. Promover negocios personales utilizando recursos tecnológicos del Ministerio para beneficio personal.

16. Impedir u obstaculizar el funcionamiento normal del acceso a la infraestructura informática, datos o redes del Ministerio sin autorización.

17. Destruir, dañar, borrar o deteriorar datos informáticos o sistemas del Ministerio.

18. Distribuir, enviar o introducir software malicioso u otros programas dañinos en la plataforma tecnológica del Ministerio.

19. Modificar o alterar datos personales en bases de datos sin autorización adecuada.

20. No mantener la confidencialidad de las contraseñas, permitiendo que otros accedan con su usuario y clave.

21. Permitir acceso u otorgar privilegios a personas no autorizadas en las redes del Ministerio.

22. Realizar actividades fraudulentas, ilegales o intentar acceder no autorizado a la infraestructura tecnológica del Ministerio.

23. Retirar equipos que contengan información institucional sin autorización previa.

24. Sustraer documentos clasificados y abandonarlos en lugares públicos o accesibles sin medidas adecuadas para su protección.

25. Entregar, enseñar o divulgar información institucional reservada a personas no autorizadas.

26. Realizar cambios no autorizados en la infraestructura tecnológica del Ministerio.

27. Instalar programas no autorizados en los equipos del Ministerio.

28. Copiar aplicaciones del Ministerio sin autorización, violando derechos de autor o acuerdos de licenciamiento.

Procedimientos Disciplinarios

Las acciones disciplinarias se llevarán a cabo conforme al Código Único Disciplinario para servidores públicos y según los criterios definidos en los contratos para contratistas. Los incidentes que constituyan delitos informáticos serán reportados a las autoridades competentes para su investigación y posible acción legal.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Nombre y Cargo: José Germán Jiménez Palomino **Fecha:** *20 de diciembre de 2024*	**Nombre y Cargo:** **Edgar Fernando Suarez Mendoza - Jorge Eliécer González Díaz.** Coordinador Grupo Seguridad de la Información e Innovación - OTIC **Fecha:** *30 de diciembre de 2024*	**Nombre y Cargo:** **Didier Anibal Beltrán Cadena**. Jefe OTIC (e) **Fecha:** *08 de mayo de 2025*