# INFORME DE SEGUIMIENTO

# MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## PRIMER TRIMESTRE 2026

## OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

## MARZO DE 2026

# CONTENIDO

# INTRODUCCIÓN

La presente actividad de seguimiento al Modelo de Seguridad y Privacidad de la Información (MSPI) del Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON, se desarrolla en el marco de los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), a través de sus guías, herramientas metodológicas y hoja de ruta para la implementación y madurez del modelo. Este ejercicio tiene como propósito evaluar el nivel de avance, cumplimiento y fortalecimiento de las capacidades institucionales en materia de gestión de la seguridad de la información, en coherencia con las políticas de Gobierno Digital.

Así mismo, el seguimiento se fundamenta en los principios y controles definidos en la norma internacional ISO/IEC 27001:2022 como referente de buenas prácticas para la gestión de riesgos de seguridad de la información, permitiendo identificar brechas, oportunidades de mejora y acciones correctivas orientadas a la protección de los activos de información. En este contexto, el informe consolida los resultados del análisis realizado, evidenciando el estado actual del MSPI en la entidad y estableciendo recomendaciones estratégicas que contribuyan a su fortalecimiento continuo y alineación con estándares nacionales e internacionales.

# 1. OBJETIVOS

## 1.1. Objetivo general

Realizar la evaluación, seguimiento y retroalimentación de implementación, avance y madurez del Modelo de Seguridad y Privacidad de la Información (MSPI) en el Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON, conforme a los lineamientos, herramientas y hoja de ruta definidos por MinTIC, así como a los requisitos y buenas prácticas establecidos en la norma ISO/IEC 27001:2022, con el fin de identificar brechas, fortalecer la gestión de la seguridad de la información y promover la mejora continua en la protección de los activos de información institucionales.

## 1.2. Objetivos específicos

- ✓ Aplicar la herramienta de autodiagnóstico definida por MinTIC para evaluar el estado actual de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad, identificando el nivel de cumplimiento frente a los componentes y dominios con sus controles establecidos.

- ✓ Analizar los resultados obtenidos en la fase de diagnóstico, con el fin de determinar brechas, riesgos y oportunidades de mejora en la gestión de la seguridad y privacidad de la información, en concordancia con los lineamientos del MSPI y la norma ISO/IEC 27001:2022.

- ✓ Establecer el nivel de madurez institucional en materia de seguridad de la información, a partir de los criterios definidos en la herramienta de autodiagnóstico, permitiendo priorizar acciones estratégicas para el fortalecimiento del modelo.

- ✓ Formular recomendaciones y acciones de mejora orientadas al cierre de brechas identificadas en la fase de diagnóstico, promoviendo la alineación del MSPI con las buenas prácticas de la norma ISO/IEC 27001:2022 y la hoja de ruta establecida por MinTIC.

## 2. METODOLOGÍA

El Modelo de Seguridad y Privacidad de la Información (MSPI) se implementa bajo un enfoque metodológico basado en la mejora continua, el cual se estructura en fases que comprenden el diagnóstico, la planificación, la implementación y el seguimiento de los controles de seguridad de la información. Este enfoque permite orientar de manera organizada las actividades necesarias para evaluar, fortalecer y mantener la gestión de la seguridad de la información, asegurando su articulación con los procesos institucionales y el cumplimiento de los lineamientos establecidos a nivel nacional.


La entidad ha realizado el diagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), a través de la aplicación del instrumento de autodiagnóstico dispuesto por MINTIC. Esta etapa ha permitido identificar el estado actual de la gestión de la seguridad de la información, así como las brechas existentes frente a los lineamientos, dominios y diferentes controles allí establecidos. Una vez finalizado este proceso, se da continuidad a la fase de planificación, en la cual se definirán las acciones, estrategias y planes de mejora necesarios para fortalecer la implementación del modelo y avanzar en su nivel de madurez.

Los dominios contemplados por esta herramienta son Organizacionales, Personales, Físicos, Tecnológicos, y sus controles correspondientes están basados en la norma ISO/IEC 27001:2022. Esta herramienta, estructurada bajo el ciclo PHVA (Planear, Hacer,

Verificar, Actuar), facilita la identificación de brechas, riesgos y oportunidades de mejora en la gestión de la seguridad de la información.

Durante el diligenciamiento de cada control se ha verificado la información basada en las evidencias relacionadas, las cuales se componen de políticas, procedimientos, formatos, entre otros.

## 3. ESTADO DE AUTODIAGNÓSTICO

Los resultados del autodiagnóstico evidencian un nivel de avance significativo en los diferentes dominios evaluados, destacándose especialmente los controles organizacionales, de personas y físicos, los cuales presentan niveles de cumplimiento cercanos al objetivo establecido. No obstante, se observa una brecha más marcada en los controles tecnológicos, lo que indica la necesidad de fortalecer este componente para lograr un equilibrio en la implementación del modelo. En términos generales, la entidad presenta una base sólida en la gestión de la seguridad de la información, con avances importantes que permiten orientar los esfuerzos hacia el cierre de brechas y la consolidación de un enfoque integral y alineado con los estándares de la ISO/IEC 27001:2022.


### 3.1 Nivel de madurez por dominios del MSPI

Durante el proceso de autodiagnóstico en IDIPRON se evidencian avances en la revisión de los cuatro dominios establecidos y actualizados en la Norma ISO/IEC 27001:2022: Organizacionales, Personas, Físicos y Tecnológicos. Cada dominio se analiza de manera sistemática a través del diligenciamiento de la herramienta y los hallazgos documentados en los controles del MSPI.

| No. | Evaluación de Efectividad de controles | | | |
|---|---|---|---|---|
| | DOMINIO | Calificación Actual (%) | Calificación Objetivo(%) | Nivel de Madurez |
| A.5 | CONTROLES ORGANIZACIONALES | 96 | 100 | **OPTIMIZADO** |
| A.6 | CONTROLES DE PERSONAS | 98 | 100 | **OPTIMIZADO** |
| A.7 | CONTROLES FÍSICOS | 90 | 100 | **OPTIMIZADO** |
| A.8 | CONTROLES TECNOLÓGICOS | 70 | 100 | **GESTIONADO** |
| **PROMEDIO EVALUACIÓN DE CONTROLES** | | **89** | **100** | **OPTIMIZADO** |

A partir de los resultados obtenidos en el autodiagnóstico, se presenta a continuación el análisis detallado por cada uno de los dominios evaluados, con el fin de evidenciar el estado actual de implementación de los controles, los avances alcanzados y los aspectos a fortalecer en cada componente del Modelo de Seguridad y Privacidad de la Información.

## 3.2 Dominios y Controles

### 3.2.1 Organizacional

Son aquellos mecanismos, políticas y procedimientos que establecen la estructura institucional, su propósito es garantizar que la seguridad de la información esté integrada en la cultura organizacional y respaldada por la alta dirección, incluyen la definición de roles y responsabilidades, la formalización de políticas, la asignación de recursos, la gestión documental y el cumplimiento normativo.

De acuerdo con los resultados del autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), el dominio organizacional en el IDIPRON evidencia un nivel importante de avance en la estructuración de los lineamientos estratégicos que orientan la gestión de la seguridad de la información, consolidándose como el eje central sobre el cual se articulan los demás dominios del modelo.

En este contexto, se destaca la existencia de la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SEGURIDAD DIGITAL – POLÍTICA – CIBERSEGURIDAD Y CIBERDEFENSA (E-GTIC-MA-001), la cual se encuentra debidamente establecida, actualizada y vigente, constituyéndose como el principal instrumento orientador para la gestión de la seguridad de la información en la entidad.

Esta política permite definir el marco general de actuación, establecer directrices claras y alinear a las diferentes dependencias en torno a los objetivos institucionales en materia de seguridad digital.

Adicionalmente, se evidencian avances en la definición de roles y responsabilidades, lo cual permite estructurar un esquema de gobernanza que facilita la toma de decisiones y el seguimiento a las actividades relacionadas con la seguridad de la información. Este aspecto es clave para garantizar la asignación de responsabilidades y promover el cumplimiento de los lineamientos establecidos en los diferentes niveles de la entidad.

Se identifican lineamientos relacionados con la gestión de riesgos y el cumplimiento normativo, los cuales contribuyen a fortalecer la capacidad institucional para identificar, analizar y tratar los riesgos asociados a la seguridad de la información. Este enfoque permite a la entidad avanzar hacia una gestión más preventiva y estructurada, alineada con los principios de la ISO/IEC 27001:2022 y con las directrices definidas por el MinTIC.

El dominio organizacional refleja la incorporación progresiva de la seguridad de la información dentro de los procesos institucionales, favoreciendo su integración con la planeación estratégica y su articulación con las diferentes áreas de la entidad. Esto permite que la seguridad de la información sea gestionada como un componente transversal, y no como un elemento aislado, fortaleciendo así su impacto en la operación institucional.

No obstante, los resultados del autodiagnóstico permiten identificar oportunidades de fortalecimiento relacionadas con la actualización y socialización continua de los lineamientos, así como con la necesidad de consolidar mecanismos de seguimiento que permitan evidenciar su implementación efectiva en todas las dependencias. Asimismo, se hace necesario continuar avanzando en la articulación entre dependencias, con el fin de garantizar una aplicación homogénea de los controles y una mayor coherencia en la gestión institucional de la seguridad de la información.

Con el propósito de fortalecer la claridad en la asignación de funciones y responsabilidades, se elaboró una matriz RACI, la cual permite identificar de manera estructurada los responsables (R), quienes aprueban (A), los consultados (C) y los informados (I) en los diferentes procesos relacionados con la seguridad de la información y contribuye a mejorar la toma de decisiones, el seguimiento de los controles y el cumplimiento de los lineamientos establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI).

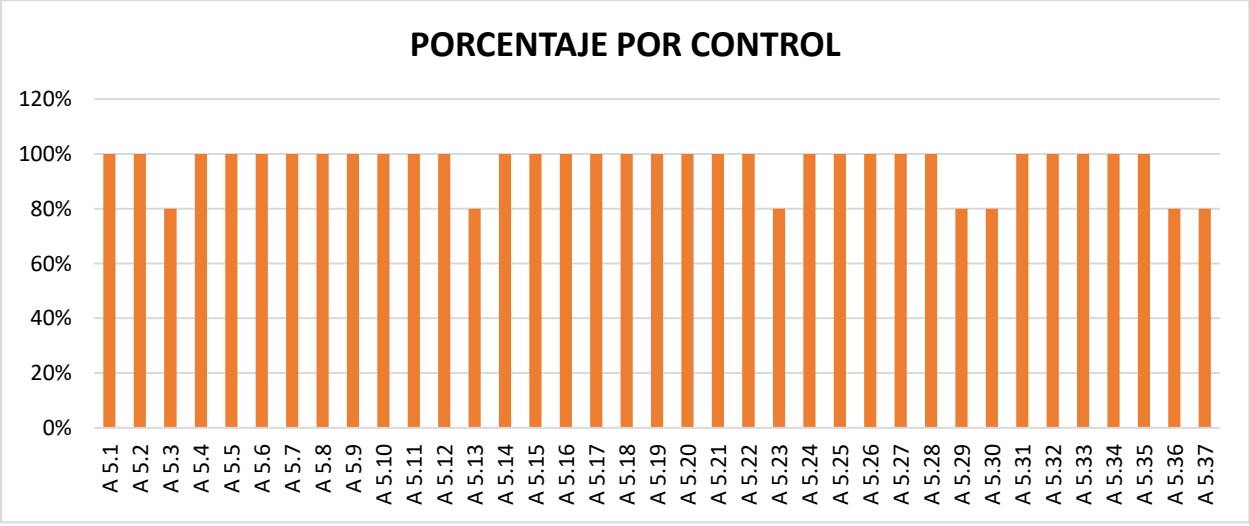
- **Matriz Raci**

| Proceso | Actividad | Alta Dirección | Jefe OTIC | Equipo Seguridad | Dueño Proceso | Auditor (Control Interno) | Usuarios |
|---|---|---|---|---|---|---|---|
| **Diagnóstico** | Aplicar autodiagnóstico MSPI | I | A | R | C | I | I |
| **Diagnóstico** | Identificación de activos | I | A | R | C | I | I |
| **Diagnóstico** | Identificación de riesgos | I | A | R | C | I | I |
| **Planificación** | Definir alcance del MSPI | A | R | R | C | I | I |
| **Planificación** | Formular políticas de seguridad | A | R | R | C | I | I |
| **Implementación** | Implementar controles de seguridad | I | A | R | C | I | I |
| **Implementación** | Gestión de activos de información | I | A | R | R/C | I | I |
| **Implementación** | Controles de acceso | I | A | R | R/C | I | R |
| **Operación** | Gestión de incidentes | I | A | R | C | I | I |
| **Operación** | Gestión de vulnerabilidades | I | A | R | C | I | I |
| **Operación** | Copias de respaldo | I | A | R | C | I | I |
| **Evaluación** | Monitoreo y control | I | A | R | C | I | I |
| **Evaluación** | Seguimiento a indicadores | A | R | R | C | I | I |
| **Mejora Continua** | Plan de mejoramiento | A | R | R | C | I | I |
| **Mejora Continua** | Lecciones aprendidas | A | R | R | C | I | I |

**Síntesis de resultados del dominio**

- **Fortalezas:** Se destaca la existencia de un marco normativo definido que orienta la gestión de la seguridad de la información en la entidad, evidenciado principalmente en la POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – SEGURIDAD DIGITAL – POLÍTICA – CIBERSEGURIDAD Y CIBERDEFENSA (E-GTIC-MA-001), la cual se encuentra establecida, actualizada y vigente. Asimismo, se identifican avances en la definición de roles y responsabilidades, así como en la estructuración de lineamientos que permiten integrar la seguridad de la información dentro de los procesos institucionales, fortaleciendo su gobernanza y alineación con los objetivos estratégicos.

- **Porcentaje de avance**: Como resultado de la evaluación de los controles (37) establecidos para el dominio organizacional en el marco del autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), se observa un nivel de cumplimiento del 96%, lo cual evidencia un desarrollo importante en la adopción de los lineamientos estratégicos de seguridad de la información en el IDIPRON. Este comportamiento refleja que la entidad ha logrado consolidar un conjunto de controles que, en su mayoría, se encuentran definidos y respaldados, permitiendo fortalecer la estructura institucional en materia de seguridad.
  En este sentido, el resultado alcanzado permite evidenciar que se han establecido elementos clave para la consolidación del Sistema de Gestión de Seguridad de la Información (SGSI), particularmente en lo relacionado con la gobernanza, la definición de políticas y la articulación de la seguridad con los procesos institucionales.



- **Beneficios:** Los avances en este dominio han permitido fortalecer la gobernanza de la seguridad de la información, facilitando la definición de lineamientos claros, la asignación de responsabilidades y la articulación entre las diferentes dependencias. Esto contribuye a una gestión más organizada y coherente, mejora la capacidad institucional para gestionar riesgos y favorece el cumplimiento de los lineamientos establecidos a nivel normativo, impactando positivamente la sostenibilidad y efectividad del MSPI.

### 3.2.2 Personas

El dominio de controles de personas en el IDIPRON presenta un nivel de cumplimiento alto, evidenciado en la implementación a su 100% de la mayoría de los controles evaluados, los cuales cuentan con soporte documental y lineamientos definidos que orientan la gestión del talento humano en materia de seguridad de la información.

En relación con los procesos de vinculación, se evidencia que la entidad cuenta con procedimientos establecidos que permiten orientar la selección del personal bajo criterios definidos, contribuyendo a la incorporación de talento humano alineado con las necesidades institucionales. Este aspecto representa un avance importante en la mitigación de riesgos asociados al acceso a la información desde etapas iniciales de la relación laboral.

La formalización de acuerdos contractuales y compromisos de confidencialidad permite establecer un marco claro de responsabilidades frente al manejo de la información, fortaleciendo la protección de los activos institucionales y promoviendo prácticas adecuadas en el desarrollo de las funciones asignadas.

En cuanto a la sensibilización y formación, la entidad ha incorporado la seguridad de la información dentro de sus estrategias de capacitación, a través del Plan Institucional de Capacitación, lo cual evidencia un avance en la generación de espacios orientados a fortalecer el conocimiento del personal.

Por otra parte, se observa que la entidad dispone de lineamientos relacionados con la gestión disciplinaria, la finalización de la relación laboral y el trabajo remoto, lo cual permite establecer un marco de control frente a diferentes situaciones que pueden afectar la seguridad de la información. Estos elementos contribuyen a la consolidación de prácticas organizacionales orientadas al cumplimiento y al uso adecuado de los recursos institucionales.

Finalmente, en lo relacionado con el reporte de eventos de seguridad de la información, si bien se cuenta con lineamientos definidos, los resultados del autodiagnóstico

evidencian la necesidad de fortalecer su difusión y apropiación por parte del personal, con el fin de asegurar una respuesta oportuna frente a posibles incidentes.

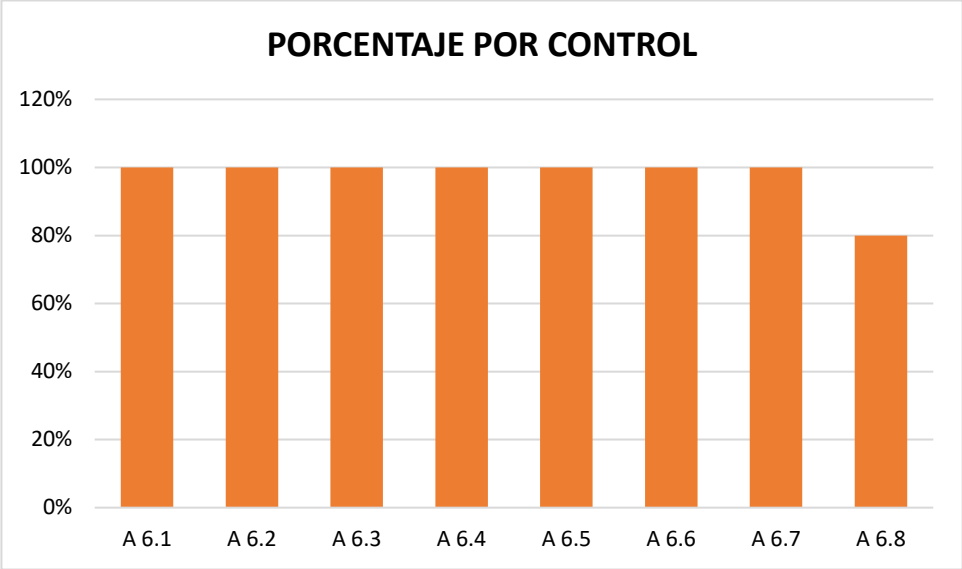
**Síntesis de resultados del dominio**

- **Fortalezas**: Se destaca la existencia de lineamientos, políticas y procedimientos formalmente establecidos que cubren el ciclo de vida del talento humano, lo cual ha permitido a la entidad contar con una base estructurada para la gestión de la seguridad de la información. Asimismo, se evidencia la implementación de controles asociados a la confidencialidad, capacitación y regulación del comportamiento del personal, lo que contribuye a la protección de los activos de información y al fortalecimiento del cumplimiento institucional.

- **Porcentaje de avance:** A partir de la evaluación de los 8 controles definidos para el dominio de personas en el marco del autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), se evidencia un nivel de cumplimiento del 98%, lo cual refleja un avance significativo en la implementación de los lineamientos asociados a la seguridad de la información en el IDIPRON. Este resultado pone de manifiesto que la entidad cuenta con controles mayoritariamente implementados y soportados, lo que evidencia un alto grado de estructuración y compromiso institucional frente a la gestión de la seguridad de la información.

  El nivel pendiente para alcanzar la totalidad refleja la necesidad de fortalecer la difusión y apropiación por parte del personal, con el fin de asegurar una respuesta oportuna frente a posibles incidentes, en coherencia con la normatividad vigente.

  De igual manera, este nivel de cumplimiento permite identificar que se han establecido bases sólidas para la consolidación del Sistema de Gestión de Seguridad de la Información (SGSI), facilitando la continuidad en su fortalecimiento y la evolución hacia niveles de madurez más gestionados.




- **Beneficios:** Los avances alcanzados en este dominio han permitido fortalecer la gestión del talento humano desde la perspectiva de la seguridad de la información, reduciendo riesgos asociados al factor humano, mejorando la claridad en las responsabilidades del personal y promoviendo una cultura organizacional orientada a la protección de la información. Esto contribuye directamente a la confiabilidad de los procesos institucionales y al adecuado manejo de la información sensible gestionada por la entidad.

### 3.2.3 Físicos

De acuerdo con los resultados del autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), el dominio de controles físicos en el IDIPRON evidencia un avance importante en la implementación de controles orientados a la protección de las instalaciones, los equipos y los activos de información frente a riesgos físicos y ambientales.

A partir de la evaluación de los controles definidos en el Anexo A.7 de la norma ISO 27001:2022, se observa que la entidad ha establecido lineamientos relacionados con la protección de las áreas físicas, el control de accesos y la gestión de los espacios donde se almacena y procesa la información. Estos elementos permiten reducir la probabilidad de accesos no autorizados y contribuyen a la protección de los activos institucionales frente a amenazas externas e internas.

En este sentido, la entidad ha avanzado en la implementación de medidas orientadas a delimitar y proteger áreas seguras, lo cual resulta fundamental para garantizar que únicamente el personal autorizado pueda acceder a zonas críticas. Este tipo de controles

fortalece la seguridad perimetral y contribuye a minimizar riesgos asociados a intrusión, manipulación indebida o pérdida de información.

Asimismo, se evidencian controles relacionados con la ubicación, protección y mantenimiento de los equipos, lo cual permite mitigar riesgos asociados a daños físicos, fallas operativas o afectaciones derivadas de condiciones ambientales. La existencia de estos lineamientos aporta a la continuidad de los servicios y a la disponibilidad de la información, elementos clave para el cumplimiento de la misión institucional.

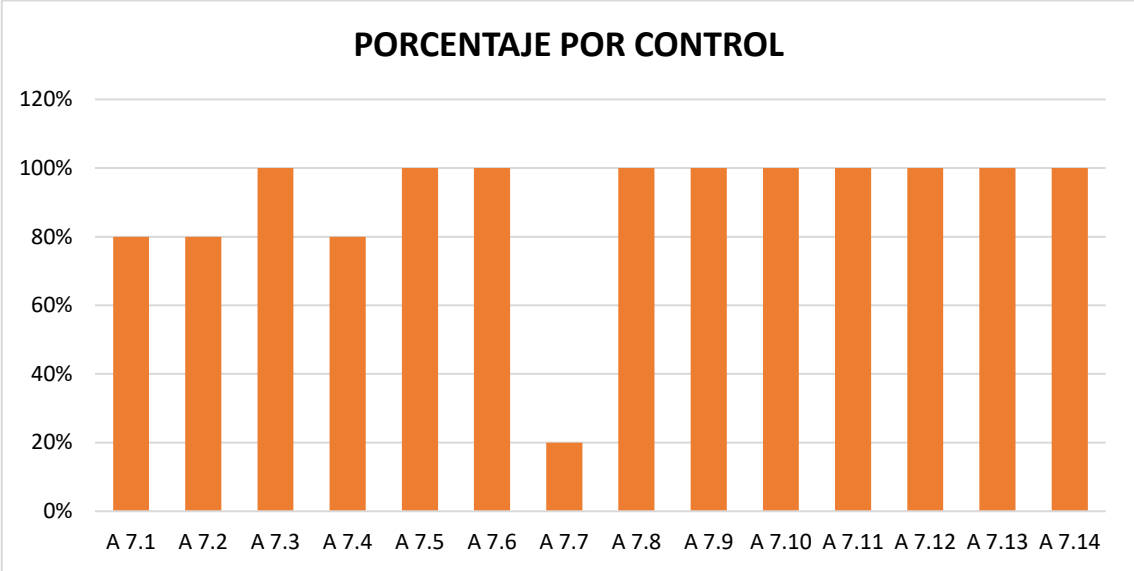
Se identifican prácticas orientadas a la gestión de riesgos ambientales, tales como la protección frente a fallas eléctricas, condiciones de temperatura y otros factores que pueden impactar la infraestructura tecnológica. Estos controles son esenciales para asegurar la estabilidad de los sistemas de información y prevenir interrupciones en la operación.

El dominio contempla controles asociados a la manipulación de activos, el retiro de equipos y la disposición segura de los mismos, lo cual contribuye a evitar la exposición de información sensible y a garantizar un manejo adecuado de los recursos institucionales a lo largo de su ciclo de vida.

No obstante, los resultados del autodiagnóstico permiten identificar que, aunque los controles se encuentran definidos y en funcionamiento, existen oportunidades de fortalecimiento relacionadas con la estandarización de algunos procedimientos, la documentación detallada de las actividades operativas y la implementación de mecanismos que permitan evidenciar de manera más clara su cumplimiento y efectividad.

- **Fortalezas**: El dominio de controles físicos evidencia la implementación de medidas orientadas al control de accesos a instalaciones y áreas críticas, lo cual permite restringir la entrada a personal no autorizado y proteger los espacios donde se encuentran ubicados los activos de información. Asimismo, se identifican lineamientos relacionados con la ubicación, protección y manejo de equipos, contribuyendo a la prevención de daños físicos y al mantenimiento de condiciones adecuadas para su funcionamiento.

- **Porcentaje de avance:** El avance en la revisión de los controles evidencia un 90% de cumplimiento, resultado del análisis de 14 controles verificados. Este progreso refleja el compromiso institucional del IDIPRON con la seguridad de la información y la consolidación del Modelo de Seguridad y Privacidad (MSPI), lo que permite fortalecer la protección de las instalaciones, los equipos y los activos de información.




- **Beneficios:** La implementación de los controles del dominio de controles físicos ha permitido fortalecer la protección de la infraestructura institucional, reducir la exposición a riesgos derivados de accesos no autorizados y minimizar la probabilidad de afectaciones a los equipos y sistemas de información. Esto contribuye directamente a la continuidad de la operación, asegurando condiciones adecuadas para el funcionamiento de los servicios y mejorando el control sobre los espacios donde se gestionan activos críticos.

### 3.2.4 Tecnológicos

Son controles implementados a través de herramientas y soluciones tecnológicas dentro del Modelo de Seguridad y Privacidad de la Información (MSPI), que permiten prevenir, detectar y mitigar riesgos sobre los activos de información (hardware y software) para proteger la información y garantizar la seguridad en los sistemas, redes y aplicaciones de la entidad. Incluyen la gestión de accesos, copias de respaldo, protección contra software malicioso, seguridad en las comunicaciones, gestión de vulnerabilidades, auditorías de sistemas y respuesta a incidentes.

En relación con la gestión de accesos a los sistemas de información, se identifican prácticas orientadas al control de privilegios y al uso de mecanismos de autenticación, lo cual evidencia un enfoque hacia la protección del acceso a los recursos tecnológicos. Estos elementos contribuyen a reducir el riesgo de accesos no autorizados y a fortalecer la seguridad en el manejo de la información institucional.

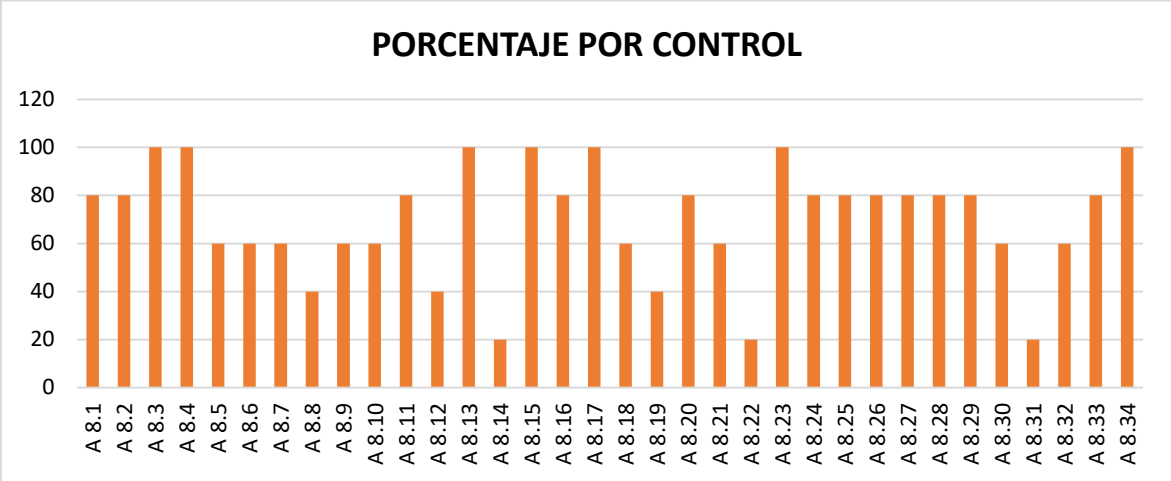
Por otra parte, frente a la protección contra amenazas tecnológicas como el software malicioso, se evidencian acciones y herramientas orientadas a la prevención y mitigación de riesgos. Estas prácticas permiten avanzar en el fortalecimiento del entorno tecnológico, favoreciendo la continuidad de los servicios y la protección de la información, en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI).

- **Fortalezas**: En IDIPRON, la gestión tecnológica se fortalece gracias a la aplicación de controles que garantizan la protección integral de la información y la continuidad de los servicios institucionales. La entidad cuenta con controles de acceso y autenticación segura, que aseguran que solo personal autorizado pueda ingresar a los sistemas; dispone de procedimientos para copias de respaldo y protección contra códigos maliciosos, lo que garantiza la recuperación de datos y la defensa frente a amenazas digitales; ha implementado medidas de seguridad en redes y comunicaciones, que refuerzan la confiabilidad de los canales de intercambio de información; y mantiene una gestión activa de vulnerabilidades técnicas, que permite anticipar riesgos y aplicar medidas correctivas oportunas.

- **Faltantes:** En IDIPRON se reconoce la importancia de avanzar en la actualización del Modelo de Seguridad y Privacidad de la Información (MSPI 2026) y en la alineación con la Norma ISO/IEC 27001:2022, lo que implica contar con la revisión y aprobación de la alta Dirección como parte esencial de la implementación. Este proceso asegura respaldo institucional y compromiso estratégico en la gestión de la seguridad de la información.
  De igual manera, se proyecta un enfoque fortalecido en la gestión de incidentes y en la definición de planes de recuperación, con el propósito de garantizar la continuidad permanente de los servicios que presta la entidad. Estas acciones permitirán responder de manera oportuna ante cualquier eventualidad, reducir riesgos operativos y mantener la confianza de los beneficiarios y de los entes de control.

- **Porcentaje de avance:** El proceso de revisión de los controles evidencia un 70% de cumplimiento, resultado del análisis de 34 controles verificados. Este avance refleja un progreso significativo en la consolidación del Modelo de Seguridad y Privacidad de la Información (MSPI), demostrando el compromiso institucional de IDIPRON con la protección de sus activos y la gestión responsable de la información.

  Este enfoque garantiza que cada hallazgo se convierta en una acción concreta de mejora, alineando la gestión institucional con los estándares de la ISO/IEC 27001:2022 y con la hoja de ruta del MinTIC.

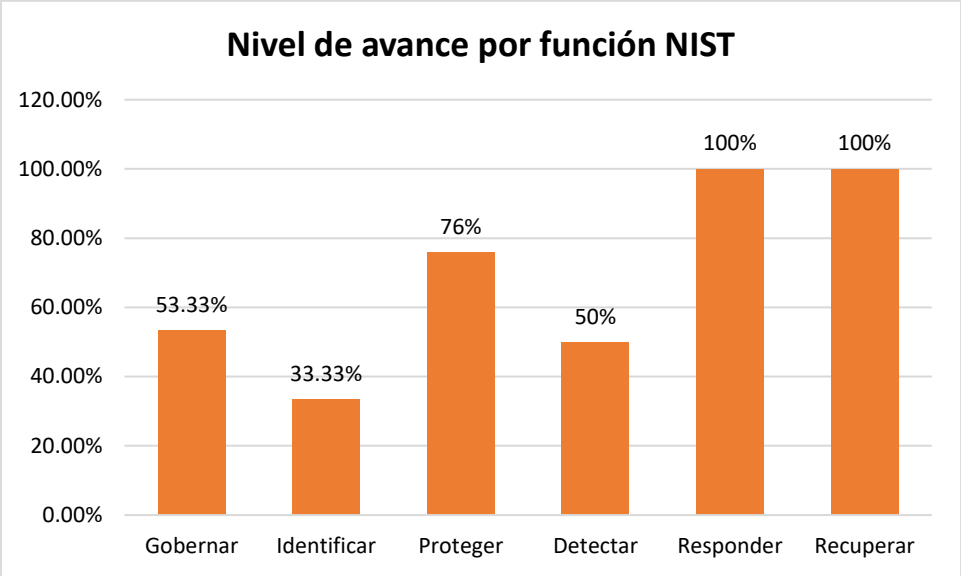



- **Beneficios:** La implementación de los controles del dominio Tecnológicos asegura que la infraestructura digital de IDIPRON funcione de manera confiable, segura y disponible en todo momento. Estos controles permiten proteger los sistemas y aplicaciones frente a amenazas, garantizar la continuidad de los servicios y mantener la integridad de la información institucional.

## 4. AVANCE

El proceso de autodiagnóstico se encuentra con un avance en la adopción del marco NIST, con un promedio general de cumplimiento del 69%. Este resultado refleja que la entidad ha iniciado la estructuración de la gestión de seguridad de la información, con avances relevantes en capacidades asociadas a la respuesta y recuperación ante incidentes, así como en la protección de los activos de información.

Los niveles de avance identificados por función son:




**Promedio total:** 68.33%

Estos resultados permiten identificar tanto avances como oportunidades de fortalecimiento. La culminación del autodiagnóstico permitirá contar con un análisis más completo, el cual servirá como base para la definición de acciones en la fase de planificación.

## 5. OPORTUNIDADES DE MEJORA

Se desarrollaron actividades orientadas al fortalecimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en el IDIPRON mediante la implementación de acciones de mejora continua basadas en el seguimiento de incidentes y revisión de indicadores de gestión.

Como resultado de este proceso, se identifican oportunidades de mejora relacionadas con la gestión de accesos, actualización de documentación. Con los hallazgos realizados, se formularán e implementarán acciones correctivas y preventivas, enfocadas en fortalecer los controles existentes y mitigar los riesgos asociados.

Se permite evidenciar la necesidad de seguir consolidando el marco organizacional que soporta la seguridad de la información, especialmente en lo relacionado con la actualización y coherencia de los lineamientos institucionales. En este sentido, resulta clave asegurar que las políticas y directrices existentes se mantengan alineadas con la

evolución de la entidad y sean integradas de manera efectiva en la dinámica de sus procesos.

Así mismo, se hace necesario fortalecer la forma en que la seguridad de la información se articula a nivel institucional, promoviendo una mayor integración entre áreas y una gestión más coordinada que evite esfuerzos aislados. Esto implica avanzar hacia un enfoque donde la seguridad no dependa únicamente de lineamientos formales, sino que esté incorporada en la gestión diaria y en la toma de decisiones.

Se identifican oportunidades orientadas a fortalecer la apropiación de los lineamientos de seguridad de la información por parte del personal, mediante estrategias de sensibilización más dinámicas y continuas. En este sentido, resulta necesario mejorar la difusión y claridad de los procedimientos para el reporte de incidentes, asegurando que sean comprendidos y aplicados por todos los colaboradores, así como implementar mecanismos de medición que permitan evaluar la efectividad de las capacitaciones y su impacto en el comportamiento organizacional.

Se requiere reforzar los controles asociados a la finalización de la relación laboral, garantizando la revocación oportuna de accesos y la adecuada gestión de los activos institucionales. Este aspecto es clave para prevenir riesgos asociados a accesos no autorizados y asegurar el cierre adecuado del ciclo de vida del personal en relación con la información.

Se evidencian oportunidades de mejora en la estandarización de los controles de acceso físico en las diferentes instalaciones, así como en la documentación de los procedimientos relacionados con la protección de áreas críticas y el manejo de equipos. En complemento, es necesario implementar mecanismos de seguimiento que permitan evidenciar la aplicación efectiva de estos controles en la operación diaria.

Adicionalmente, se recomienda fortalecer la gestión de riesgos asociados a condiciones ambientales, garantizando entornos adecuados para la infraestructura tecnológica, así como promover una mayor sensibilización del personal frente al cumplimiento de los controles físicos, entendiendo su rol dentro de la seguridad integral de la información.

## 6. LECCIONES APRENDIDAS

En el marco de las actividades de seguimiento del MSPI, se identifican diversas lecciones aprendidas derivadas de revisiones de procesos realizadas durante el autodiagnóstico.

Se identifica que la existencia de políticas y estructuras de gobernanza constituye la base para la gestión de la seguridad de la información, siendo determinante su integración con los procesos institucionales para asegurar una implementación coherente y alineada con los objetivos estratégicos.

Se evidencia la importancia de fortalecer la asignación y revisión periódica de permisos de acceso, así como la necesidad de mejorar la oportunidad en la atención de incidentes de seguridad. Asimismo, se identifica la relevancia de continuar promoviendo la sensibilización de los usuarios en temas de seguridad de la información, con el fin de reducir riesgos asociados a prácticas inadecuadas.

Por otra parte, se determinó la necesidad de mantener actualizada la documentación institucional, garantizando su alineación con los procedimientos operativos y los lineamientos vigentes, se integran en los planes de mejora definidos, contribuyendo al fortalecimiento continuo del MSPI.

Se reconoce que la gestión de la seguridad de la información depende en gran medida del comportamiento y nivel de apropiación del personal, evidenciando que no basta con contar con lineamientos definidos, sino que es fundamental lograr su interiorización para garantizar su aplicación efectiva en la operación diaria.

Se evidencia que la protección de la información no se limita a controles tecnológicos, sino que requiere condiciones físicas adecuadas y controladas, donde la infraestructura y los entornos juegan un papel clave en la prevención de riesgos y en la continuidad de los servicios.

El diligenciamiento periódico y oportuno de la matriz de diagnóstico permitirá mantener una visión actualizada del nivel de madurez del MSPI, facilitando la identificación temprana de brechas y la toma de acciones correctivas para asegurar su mejora continua, en alineación con ISO/IEC 27001:2022.

## 7. CONCLUSIONES

El seguimiento realizado al Modelo de Seguridad y Privacidad de la Información (MSPI) en IDIPRON durante el primer trimestre de 2026 refleja avances significativos en la consolidación de prácticas sólidas de gestión de la seguridad de la información. La entidad ha demostrado capacidad para proteger sus activos institucionales, alineándose con las mejores prácticas internacionales y con el marco de referencia NIST, bajo la metodología del ciclo PHVA (Planear, Hacer, Verificar, Actuar).

En el IDIPRON se evidencia un nivel importante de consolidación en la definición de los lineamientos que orientan la gestión de la seguridad de la información, permitiendo establecer una base estructurada para su desarrollo a nivel institucional. La existencia de políticas, roles y directrices facilita la articulación de la seguridad con los procesos de la entidad y fortalece su enfoque estratégico.

El desarrollo del dominio de personas dentro del MSPI ha contribuido a que IDIPRON cuente con una base sólida para la gestión de la seguridad de la información, permitiendo reducir riesgos asociados al factor humano, mejorar la claridad en las responsabilidades

del personal y avanzar en la construcción de una cultura organizacional orientada a la protección de la información

Se identifica la necesidad de continuar fortaleciendo la apropiación de estos controles por parte del personal, promoviendo una mayor conciencia sobre la importancia de la seguridad física como un componente integral de la seguridad de la información. Esto resulta clave para asegurar que las medidas establecidas no solo existan a nivel documental, sino que sean aplicadas de manera consistente en la operación diaria.

El dominio del control físico en el IDIPRON refleja un nivel relevante de consolidación en la protección de su infraestructura y de los entornos donde se soporta la operación institucional, evidenciando la existencia de controles que permiten gestionar el acceso a las instalaciones, resguardar áreas sensibles y mantener condiciones adecuadas para el funcionamiento de los equipos. Estos avances aportan a la estabilidad operativa y al resguardo de los activos de información; sin embargo, es importante seguir avanzando en la uniformidad de su aplicación y en el fortalecimiento de los mecanismos que permitan garantizar su cumplimiento en todas las sedes y contextos de la entidad.

Para terminar, es importante resaltar que la entidad ha adelantado la fase de diagnóstico mediante la aplicación del autodiagnóstico del MSPI, lo cual ha permitido identificar el estado actual de la seguridad de la información y las principales brechas existentes. En este contexto, el siguiente paso corresponde a la fase de planificación, en la cual se definirán las acciones y estrategias necesarias para fortalecer la implementación del modelo y avanzar en su nivel de madurez.

Finalmente es importante dar continuidad al compromiso de la Alta Dirección, con la implementación, sostenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad, garantizando la asignación de recursos, el fortalecimiento de las capacidades tecnológicas institucionales y el liderazgo necesario para consolidar una cultura organizacional orientada a la protección de la información y la gestión adecuada de los riesgos, en alineación con las buenas prácticas establecidas por MINTIC a través de las Políticas de Gobierno Digital y Seguridad Digital

Firma: 

Nombre: Andrea Carolina Cruz Omaña

**Jefe OTIC**

Firma: 

Nombre: Edgar Antonio Carreño Chaparro

Contratista Profesional