PROCESO DIRECCIONAMIENTO ESTRATÉGICO TIC

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Corporación Autónoma del Tolima reconoce la creciente exposición de las entidades públicas a incidentes de seguridad digital que pueden impactar su funcionamiento y la prestación de servicios a la ciudadanía. En este contexto, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece lineamientos para diseñar, adoptar y promover políticas en el uso y apropiación de las TIC, con el objetivo de gene rar confianza en el entorno digital.

La política de gobierno digital busca promover lineamientos en el uso de las TIC, garantizando la seguridad y privacidad de la información como habilitador transversal. Este enfoque busca asegurar eficientemente trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física, gestionando activos de información y evitando interrupciones en la prestación de servicios.

1.1. Modelo de Seguridad y Privacidad de la Información (MSPI)

El MinTIC ha desarrollado el Modelo de Seguridad y Privacidad de la Información (MSPI), que define lineamientos para la implementación de la estrategia de seguridad digital. Este modelo se basa en un ciclo PHVA (Planear, Hacer, Verificar y Actuar) e incluye aspectos legales, técnicos, normativos y reglamentarios. Consta de cinco fases:

1.1.1. **Diagnóstico**:

- Iniciar con un análisis GAP para identificar el estado actual de la entidad respecto a la adopción del MSPI.

INFORME DE VULNERABILIDADES EN PUERTOS ABIERTOS DEL SERVIDOR

Resumen Ejecutivo:

Este informe ejecutivo tiene como objetivo proporcionar una evaluación de seguridad detallada del servidor con dirección **IP 192.168.20.1, 192.168.20.5, 192.168.20.6, 192.168.20.7, 192.168.20.9, 192.168.20.10, 192.168.20.11, 192.168.20.15, 192.168.20.22, 192.168.20.23, 192.168.20.35, 192.168.20.36**. analizando e identificando vulnerabilidades y posibles riesgos en varios puertos y servicios. Las recomendaciones incluyen actualizaciones de software, configuraciones de seguridad y evaluación de aplicaciones web. Es

esencial tomar medidas inmediatas para mitigar las vulnerabilidades y fortalecer la seguridad del servidor acorde a lo realizado.

1.1.2. Planificación:

Se determinaron objetivos y límites de seguridad para la privacidad de la información considerando el mapa de procesos, tamaño y contexto interno y externo.

Objetivo del Modelo de Seguridad y Privacidad de la Información

El objetivo del Modelo de Seguridad y Privacidad de la Información (MSPI) de CORTOLIMA es establecer un marco de gestión que garantice la protección efectiva de la información crítica y sensible de la entidad, asegurando su confidencialidad, integridad y disponibilidad. Dentro de esta se busca identificar, evaluar y mitigar los riesgos asociados a la seguridad y privacidad de la información, promoviendo una cultura organizacional consciente de la importancia de la seguridad de la información y el cumplimiento de la normativa aplicable en materia de protección de datos y seguridad de la información.

Límites del Modelo de Seguridad y Privacidad de la Información

Los límites del MSPI están definidos por la naturaleza de la información que CORTOLIMA gestiona y su aplicabilidad se restringe a las operaciones y jurisdicción de la entidad. No abarca la seguridad y privacidad de la información fuera del control operativo de CORTOLIMA o aquella gestionada por entidades externas, a menos que exista un acuerdo formal que especifique lo contrario. Además, el MSPI se enfoca en la gestión de la seguridad y privacidad de la información, excluyendo otros aspectos de seguridad no relacionados directamente con la información, como la seguridad física general de las instalaciones y el control de acceso del personal interno y externo, a menos que dichos aspectos incidan directamente con la seguridad de la información.

Se definió un plan de valoración y tratamiento de riesgos como parte crucial del ciclo

Plan de Valoración y Tratamiento de Riesgos

Se identificar los posibles riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información crítica y sensible requiriendo la toma de acciones que mitiguen los riesgos, y para esto re requiere:

- Realizar un inventario de los activos de información.
- Identificar las amenazas potenciales (internas y externas) para cada activo.
- Documentar las vulnerabilidades que pueden ser explotadas por estas amenazas.
- Entrevistas con el personal clave.
- Análisis de incidentes pasados.
- Evaluación de sistemas y redes.

Ya después de identificar posibles riesgos se realizará la evaluación de regos con el objetivo de evaluar el impacto y la probabilidad de ocurrencia de cada riesgo identificado. Y para esto se toma las siguientes acciones.

- Clasificar los riesgos en términos de impacto (bajo, medio, alto) y probabilidad (baja, media, alta).
- Priorizar los riesgos en base a su impacto y probabilidad combinados.
- Matrices de riesgo.
- Métodos cualitativos y cuantitativos de análisis de riesgos.

1.1.3. Operación:

Se implementarán controles para la mitigación y tratamiento de riesgos, con el objetivo de reducir el impacto o la probabilidad de ocurrencia de los riesgos identificados durante la fase de planificación. Se desarrollan y aplican estrategias para mitigar o tratar los riesgos identificados y evaluados.

- Seleccionar las medidas de control adecuadas (técnicas, administrativas, físicas) para reducir los riesgos.
- Implementar políticas y procedimientos de seguridad de la información.
- Capacitar al personal en prácticas de seguridad y privacidad de la información.
- Desarrollar planes de contingencia y recuperación ante desastres.
- Controles de acceso.
- Encriptación de datos.

- Sistemas de detección de intrusos.
- Planes de formación y concienciación.

1.1.4. Evaluación de Desempeño:

Se determinaron formas de evaluar la adopción del modelo.

Para evaluar la adopción de un modelo de privacidad y seguridad de la información se pueden utilizar auditorías y evaluaciones regulares estas incluyen auditorías internas y externas para evaluar la conformidad con las políticas de seguridad y privacidad establecidas y evaluaciones de riesgo para identificar y analizar los riesgos potenciales para la información y cómo se están gestionando.

1.1.5. Mejoramiento Continuo:

Se establecerán procedimientos para identificar desviaciones en las reglas definidas en el modelo.

Se realizarán encuestas para obtener una retroalimentación de los empleados a través de encuestas de conciencia de seguridad para evaluar el conocimiento y la conciencia de los empleados sobre las políticas de privacidad y seguridad y sondeos de satisfacción para obtener retroalimentación sobre la percepción de los empleados respecto a las medidas de seguridad implementadas.

Implementación de acciones correctivas y preventivas para solucionar desviaciones y evitar su repetición.

- Realizar pruebas de seguridad y evaluaciones técnicas, como las pruebas de penetración para identificar vulnerabilidades en los sistemas y las evaluaciones de vulnerabilidades usando herramientas automatizadas también son esenciales.
- Monitoreo y analizar logs de seguridad para detectar patrones inusuales o actividades sospechosas y el uso de sistemas de gestión de información y eventos de seguridad (SIEM) para centralizar y analizar los datos de seguridad son cruciales.

- Evaluar el cumplimiento normativo y legal revisando el cumplimiento con regulaciones y normativas aplicables y obtener y mantener certificaciones relevantes como ISO/IEC 27001.
- Capacitación a través de programas de seguridad y privacidad y la realización de simulaciones de incidentes y ejercicios de respuesta para evaluar la preparación del personal son fundamentales.
- Revisión de políticas y procedimientos asegura que las políticas de seguridad se actualizan regularmente y los procedimientos operativos siguen estas políticas establecidas.

2. ALCANCE

Este documento está dirigido a todos los procesos, funcionarios , usuarios y proveedores de servicios relacionados con la Política de Gobierno Digital y la estrategia de seguridad digital. Les invitamos a adoptar el Modelo de Seguridad y Privacidad de la Información en el contexto de las operaciones de la Corporación Autónoma Regional del Tolima (Cortolima) y otras iniciativas pertinentes.

3. DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados, aplicable a la Corporación Autónoma Regional del Tolima (Cortolima) (Ley 1712 de 2014, art. 4).

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización en el contexto de Cortolima (ISO/IEC 27000).
- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de Cortolima,

considerando la normativa del CONPES 3854 de 20116.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura en el ámbito de Cortolima (Ley 594 de 2000, art. 3).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización en el contexto de Cortolima (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo en las operaciones de Cortolima (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y determinar el grado en el que se cumplen los criterios de auditoría en el ámbito de Cortolima (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales en el contexto de Cortolima (Ley 1581 de 2012, art. 3).
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento en el ámbito de Cortolima (Ley 1581 de 2012, art. 3).
- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados en el contexto de Cortolima.
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios, considerando la Resolución CRC 2258 de 2009 en Cortolima.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido en el ámbito de Cortolima. Control es también utilizado como sinónimo de salvaguarda o contramedida, y en una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos en el contexto de Cortolima (Ley 1712 de 2014, art. 6).
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables en el ámbito de Cortolima (Ley 1581 de 2012, art. 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible en el ámbito de Cortolima. Son considerados datos públicos,Datos Personales Privados: Es el dato que, por su naturaleza íntima o reservada, solo es relevante para el titular en el ámbito de Cortolima (Ley 1581 de 2012, art. 3 literal h).
- **Datos Personales Mixtos:** Para efectos de este documento, es la información que contiene datos personales públicos junto con datos privados o sensibles en el contexto de Cortolima.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar discriminación. Ejemplos incluyen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (Decreto 1377 de 2013, art. 3).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad. Esto permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural, según la jurisprudencia de la Corte Constitucional.
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el Tratamiento de datos personales por cuenta del responsable del Tratamiento en Cortolima (Ley 1581 de 2012, art. 3).

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información en el ámbito de Cortolima (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que, estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica. Su acceso puede ser negado o exceptuado, siempre que se trate de circunstancias legítimas y necesarias, y respetando los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014 (Ley 1712 de 2014, art. 6).
- **Información Pública Reservada:** Es aquella información que, estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo el cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014 (Ley 1712 de 2014, art. 6).
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con las que cuenta Cortolima para ofrecer protección a los datos personales de los titulares, tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro en el ámbito de Cortolima (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para protegerla en Cortolima (ISO/IEC 27000).
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país, según la Ley 1581 de 2012, artículo 25.
- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual, a petición de la Superintendencia de Industria y Comercio, deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas

apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decide sobre la base de datos y/o el Tratamiento de los datos en Cortolima (Ley 1581 de 2012, art. 3).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias en Cortolima (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información en cualquier medio, ya sea impreso o digital, en Cortolima (ISO/IEC 27000).
- **Seguridad digital:** Preservación de la confidencialidad, integridad y disponibilidad de la información que se encuentra en medios digitales en Cortolima.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento en Cortolima (Ley 1581 de 2012, art. 3).
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión en Cortolima (Ley 1581 de 2012, art. 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad en Cortolima (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas en Cortolima (ISO/IEC 27000).
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad en Cortolima.

4. PROPÓSITOS

4.1. Propósitos del Modelo de Seguridad y Privacidad de la Información (MSPI)

El MSPI tiene como propósitos fundamentales:

4.1.1. Facilitar la Adopción y Apropiación:
Proporcionar a la entidad mecanismos, lineamientos e instrumentos de implementación claros para que puedan adoptar, implementar y apropiar el MSPI con mayor facilidad.

4.1.2. Apoyo a la Estrategia de Seguridad Digital:
Contribuir al desarrollo e implementación de la estrategia de seguridad digital de la entidad, fortaleciendo sus capacidades y medidas de seguridad.

4.1.3. Fortalecimiento de la Política de Gobierno Digital:
Establecer procedimientos de seguridad que permitan a la entidad integrar el habilitador de seguridad en la política de Gobierno Digital, consolidando así la seguridad y privacidad de la información en sus operaciones.

4.1.4. Institucionalización en Procesos y Procedimientos:
Institucionalizar la seguridad y privacidad de la información en los procesos y procedimientos de la entidad, garantizando una integración orgánica y eficaz de los principios de seguridad.

4.1.5. Contribución a la Transparencia en la Gestión Pública:
Mediante la implementación eficiente, eficaz y efectiva del MSPI, se busca contribuir al incremento de la transparencia en la gestión pública, asegurando la integridad y confidencialidad de la información.

4.1.6. Apoyo al Plan Estratégico Institucional:
Contribuir en el desarrollo y ejecución del plan estratégico institucional a través del plan de seguridad y privacidad de la información, asegurando la alineación de los objetivos de seguridad con los objetivos generales de la entidad.

5. BASE LEGAL

Conforme con lo establecido en la normatividad vigente, la Corporación Autónoma Regional del Tolima - CORTOLIMA, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la entidad:

La Constitución Política de Colombia, en su Artículo 15, establece los fundamentos legales para diversas disposiciones relacionadas con la protección de datos y la transparencia institucional. Los Artículos 209 y 269 complementan este marco constitucional, ampliando las bases jurídicas.

La Ley 1581 de 2012 se erige como una pieza clave al dictar disposiciones generales para la protección de datos personales. A su vez, el Decreto 2609 de 2012 reglamenta el Título V de la Ley 594 de 2000, abordando aspectos cruciales de la gestión documental para todas las entidades del Estado. El Decreto 1377 de 2013 complementa esta normativa al reglamentar parcialmente la Ley 1581 de 2012.

En sintonía, el Decreto 886 de 2014 reglamenta el Registro Nacional de Bases de Datos, proporcionando herramientas clave en el ámbito de la información. La Ley 1712 de 2014 entra en escena al crear la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

El Decreto 103 de 2015 y el Decreto 1074 de 2015, reglamentario del Sector Comercio, Industria y Turismo, amplían las disposiciones, vinculando la protección de datos con instrucciones específicas sobre el Registro Nacional de Bases de Datos.

El Decreto 1078 de 2015 consolida estas normativas al expedir el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Similarmente, el Decreto 1080 de 2015 y el Decreto 1081 de 2015, reglamentarios de los sectores Cultura y Presidencia, respectivamente, establecen políticas integrales de Gestión y Desempeño Institucional.

Dentro de estas políticas, el Decreto 1083 de 2015 destaca las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital". El CONPES 3854 de 2016 introduce la Política Nacional de Seguridad Digital, guiando los esfuerzos a nivel nacional.

El Decreto 728 de 2017 y el Decreto 1499 de 2017 suman capítulos emocionantes al fortalecer el modelo de Gobierno Digital y modificar disposiciones relativas al Sistema de Gestión en el Sector Función Pública.

El Decreto 1008 del 2018 establece lineamientos generales de la política de Gobierno

Digital, redefiniendo aspectos clave del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

La Ley 1915 de 2018 introduce modificaciones sustanciales en la Ley 23 de 1982, abordando cuestiones relativas a derechos de autor y conexos. El Decreto 612 de 2018 fija directrices para la integración de planes institucionales y estratégicos al Plan de Acción de las entidades del Estado.

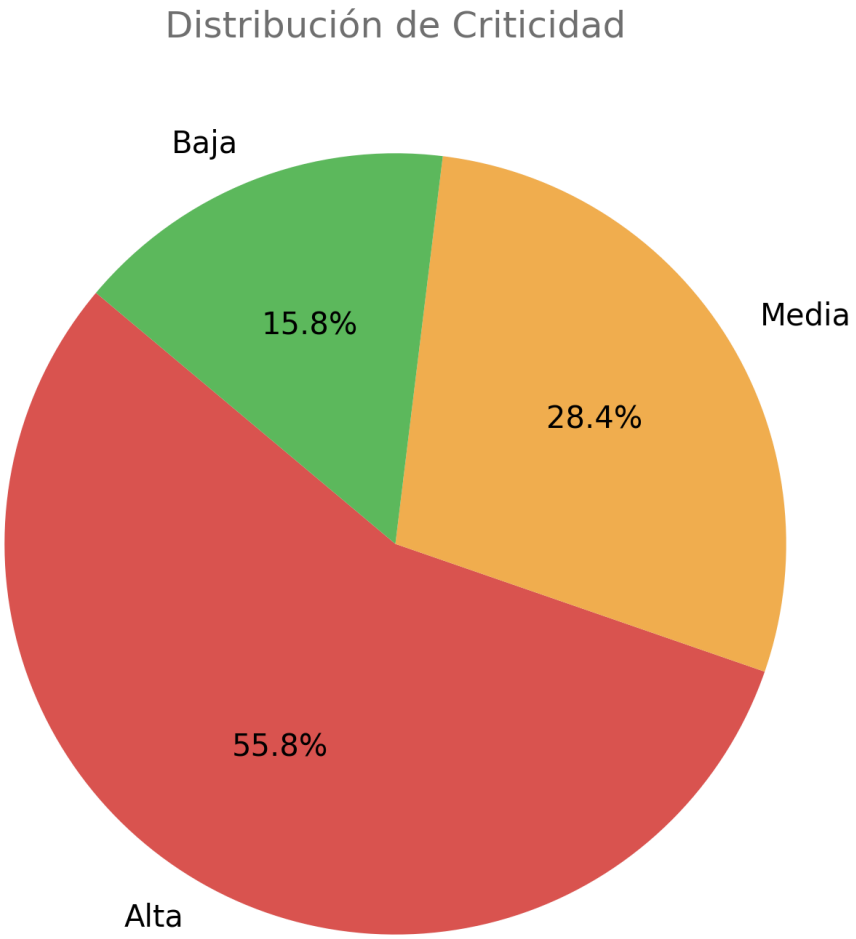
Mirando hacia el futuro digital, el Decreto 2106 de 2019 establece que las autoridades que realicen trámites digitales deben disponer de una estrategia de seguridad digital. Finalmente, la Ley 1952 de 2019 expide el Código General Disciplinario, cerrando este compendio normativo con un toque disciplinario.

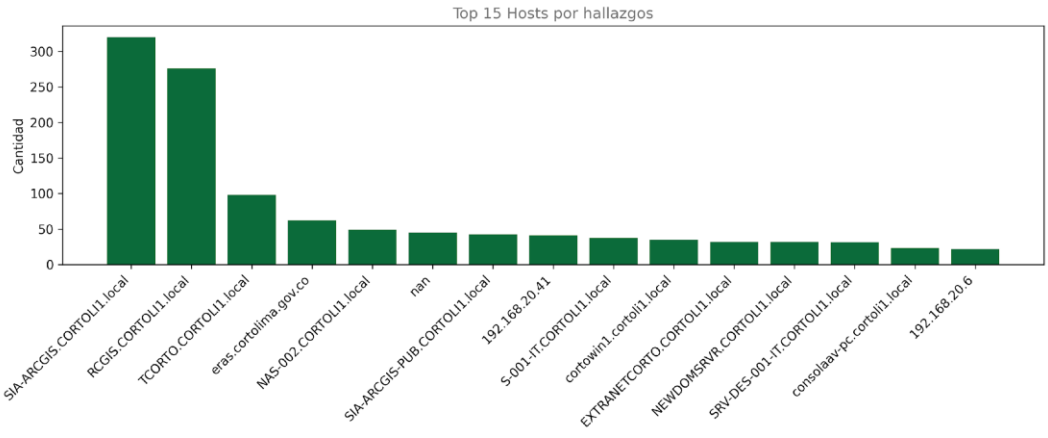
Finalmente, el presente modelo esta alineado Alineado con MSPI, Política de Gobierno Digital, MIPG y Ley 1581/2012; enfoque de defensa en profundidad, principio de mínimo privilegio, privacidad por diseño y mejora continua.

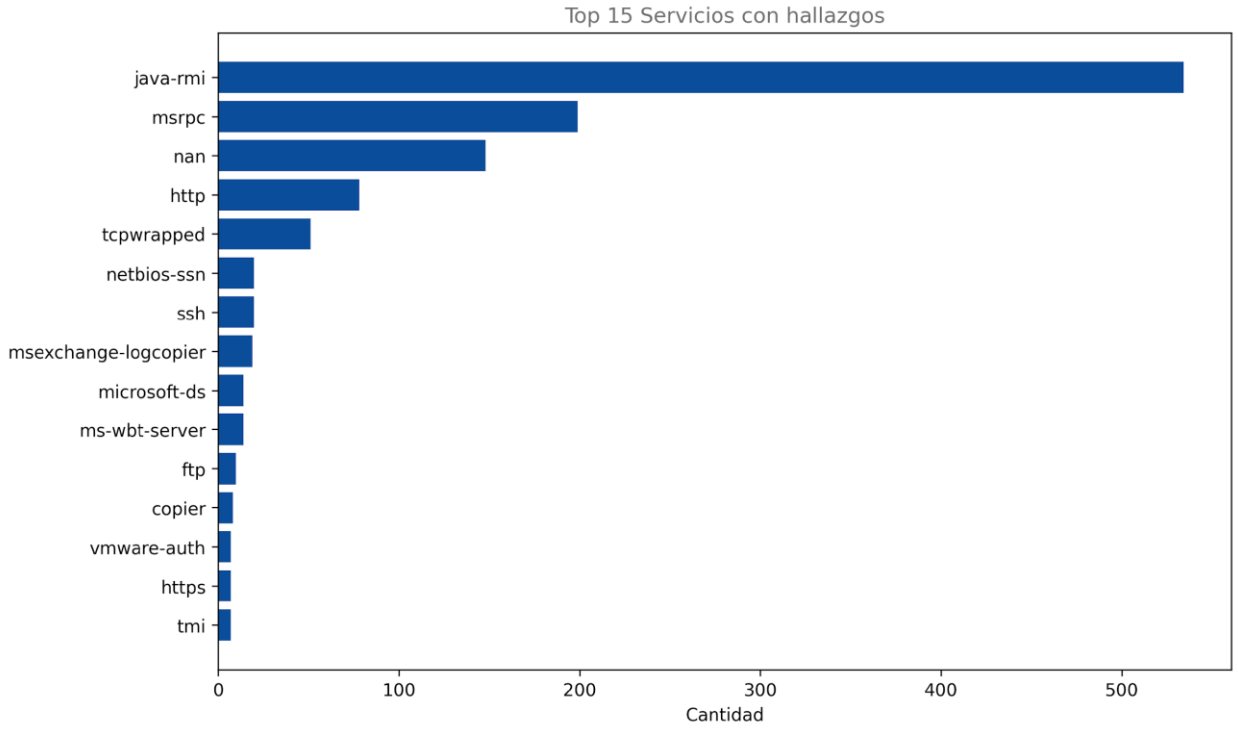
6. Infraestructura actual y arquitectura objetivo por capas

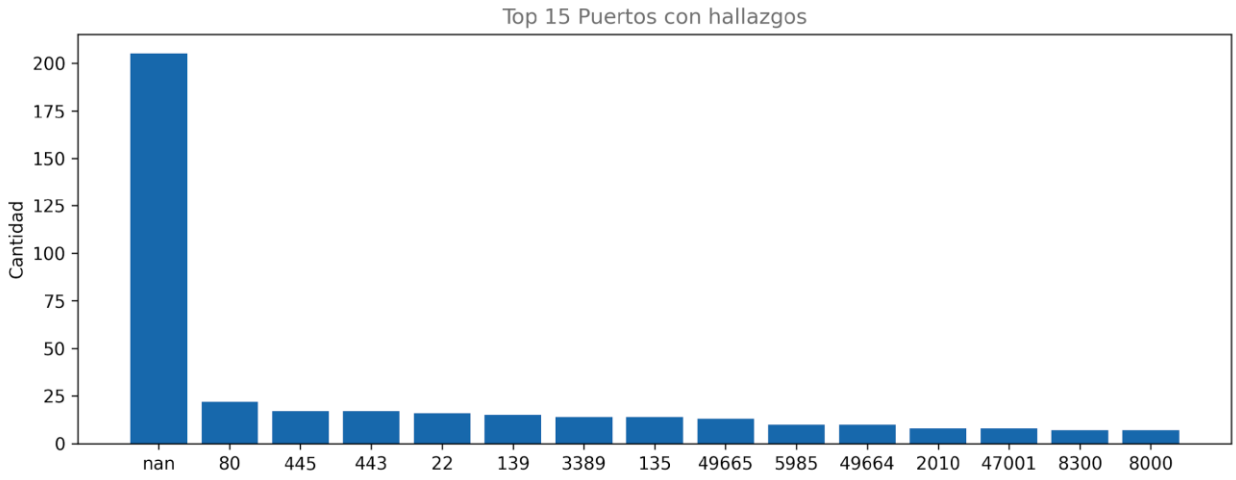
Vista actual (on-premises, virtualización, servicios publicados, DB, accesos remotos) y objetivo por capas. Diagrama conceptual:

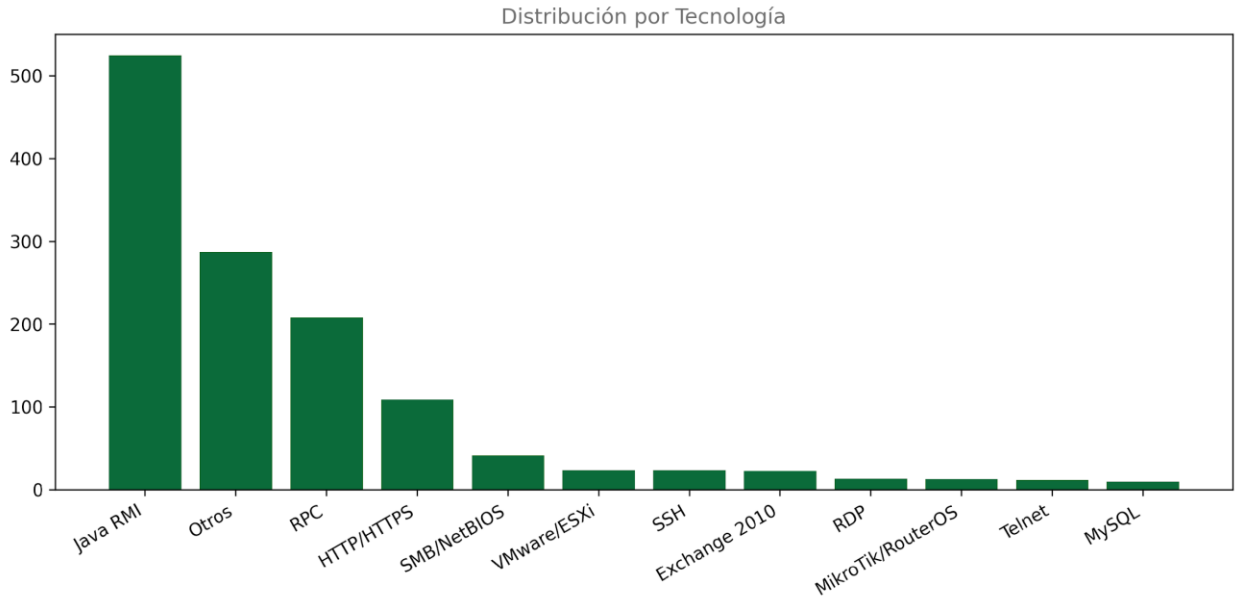
7. Diagnóstico técnico y resultados del análisis











Inventario técnico (muestra)

Host	IP	Puerto	Protocolo	Servicio	Producto	Version	SO	Criticidad
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			nan
nan		nan	nan	nan	nan			Alta
nan		nan	nan	nan	nan			Alta
nan		nan	nan	nan	nan			Media

(Mostrando 22 filas; ver Excel anexo)

8. Plan de acción priorizado (0–7 / 8–30 / 31–90 días)

Se prioriza por criticidad y exposición. Cada acción incluye horizonte sugerido, responsable editable y estado.

Backlog operativo (extracto)

Host	Servicio	Puerto	Tecnologia	Prioridad	Acción 0–7 días	Acción 8–30 días	Acción 31–90 días	Plazo sugerido	Responsable	Estado	Criticidad
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar	≤90 días	Por asignar	nan	nan

							monitoreo				
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar	≤90 días	Por asignar	nan	nan

							monitoreo				
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	nan
nan	nan	nan	Otros	Alta	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	Alta
nan	nan	nan	Otros	Alta	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	Alta
nan	nan	nan	Otros	Media	Aislar/parchear	Hardening/segmentación	Automatizar monitoreo	≤90 días	Por asignar	nan	Media

(Mostrando 22 filas; ver Excel anexo)

Resumen por Host y Prioridad

Host	Alta	Baja	Media
192.168.20.11	0	0	11
192.168.20.2	3	4	7
192.168.20.223	0	0	10
192.168.20.28	3	2	6
192.168.20.35	0	0	12
192.168.20.36	0	0	11
192.168.20.41	6	12	23
192.168.20.6	6	8	8
192.168.20.7	4	4	6
EXTRANETCORTO.CORTOLI1.local	7	0	25
NAS-002.CORTOLI1.local	6	17	26
NEWDOMSRVR.CORTOLI1.local	6	8	18
RCGIS.CORTOLI1.local	256	19	1
S-001-IT.CORTOLI1.local	10	6	21
SIA-ARCGIS-PUB.CORTOLI1.local	9	10	23
SIA-ARCGIS.CORTOLI1.local	275	27	18
SRV-DES-001-IT.CORTOLI1.local	10	4	17
TCORTO.CORTOLI1.local	11	25	62
carteleras.cortolima.gov.co	4	5	4
consolaav-pc.cortoli1.local	5	4	14
cortowin1.cortoli1.local	8	3	24
eras.cortolima.gov.co	11	20	31

(Mostrando 22 filas; ver Excel anexo)

Resumen por Servicio y Prioridad

Servicio	Alta	Baja	Media
-	0	1	0
bandwidth-test	0	2	0
cadlock	0	1	0
casrmagent	0	3	0
conf	0	2	0
copier	0	8	0
domain	0	6	0
domain-s	0	1	0
ecmp	0	1	0
elasticsearch	0	1	0
empowerid	0	1	0
flexlm	0	4	0
ftp	10	0	0
g-data-sec	0	3	0
glrpc	0	0	2
gue	0	1	0
hosts2-ns	0	2	0
http	8	0	70
http-alt	0	0	7
https	0	0	7
i-net-2000-npr	0	1	0
imap	0	2	0

(Mostrando 22 filas; ver Excel anexo)

9. MSPI por capas – Detalle y paso a paso

Perímetro/Red (UTM, segmentación, VPN)

• Cerrar exposición innecesaria (RDP/SMB/RPC/RMI).
• Implementar UTM en alta disponibilidad con IPS/Geo-blocking.
• Microsegmentación por función/criticidad; VLANs y listas de control.
• VPN con MFA; Zero-Trust para accesos administrativos.

Identidad y Accesos (MFA/SSO/PAM)

• MFA universal (administradores y personal sensible).
• Reforzar AD: contraseñas robustas/rotación, control de delegaciones.
• PAM para cuentas privilegiadas; sesiones grabadas.
• SSO OIDC/SAML y hardening de Kerberos/NTLM.

Endpoints/Servidores (EDR/Hardening)

• Cobertura EDR WithSecure 100% en críticos; políticas de aislamiento.
• Baseline de hardening (Windows/Linux/ESXi) y control de aplicaciones.
• Gestión de parches mensuales y fuera de banda para críticas.
• Backups 3-2-1 cifrados; pruebas de restauración trimestrales.

Aplicaciones (WAF/DevSecOps)

• WAF delante de portales críticos; TLS1.2+ HSTS/CSP.
• Pipeline DevSecOps (SAST/DAST/Secret scanning).
• Gestión de dependencias (SBOM) y revisión de terceros.
• Pentest anual y tras cambios mayores.

Datos (DLP/Cifrado/Clasificación)

• Clasificación de información; cifrado en reposo y tránsito.
• DLP para e-mail/web y registros de acceso a datos sensibles.
• Mascaramiento y retención; anonimización cuando aplique.
• RNBD y cumplimiento Ley 1581 (ARCO, avisos, consentimientos).

Nube e Integraciones

• Evaluación de postura (CSPM) y control de identidades (CIEM).
• Segregación de cuentas/proyectos por entorno y mínimo privilegio.
• Cifrado KMS/CMK y registros centralizados.
• Acuerdos y revisiones de proveedores (SLA/DR y seguridad).

Monitoreo, Detección y Respuesta (SIEM/IDS/EDR)

- Centralizar logs en SIEM; casos de uso (ransomware, exfiltración, brute force).
- IDS/IPS en puntos estratégicos; honeypots discretos.
- Playbooks de respuesta (CSIRT): contención, erradicación, recuperación.
- Métricas MTTD/MTTR y reporte ejecutivo mensual.

Gobierno y Cumplimiento

- Política MSPI y roles (Comité de Seguridad).
- Gestión de riesgos, auditorías internas y plan de concienciación.
- Cuadro de mando (KPIs) y revisión trimestral.
- Alineación con MSPI/Gobierno Digital/MIPG y Ley 1581/2012.

10. Análisis de soluciones y proveedores (OSS vs. Comercial)

De acuerdo a las distintas alternativas y soluciones en el mercado, se realizará dicho estudio y con base en eso se definirán los recursos requeridos para su proyección para su implementación.

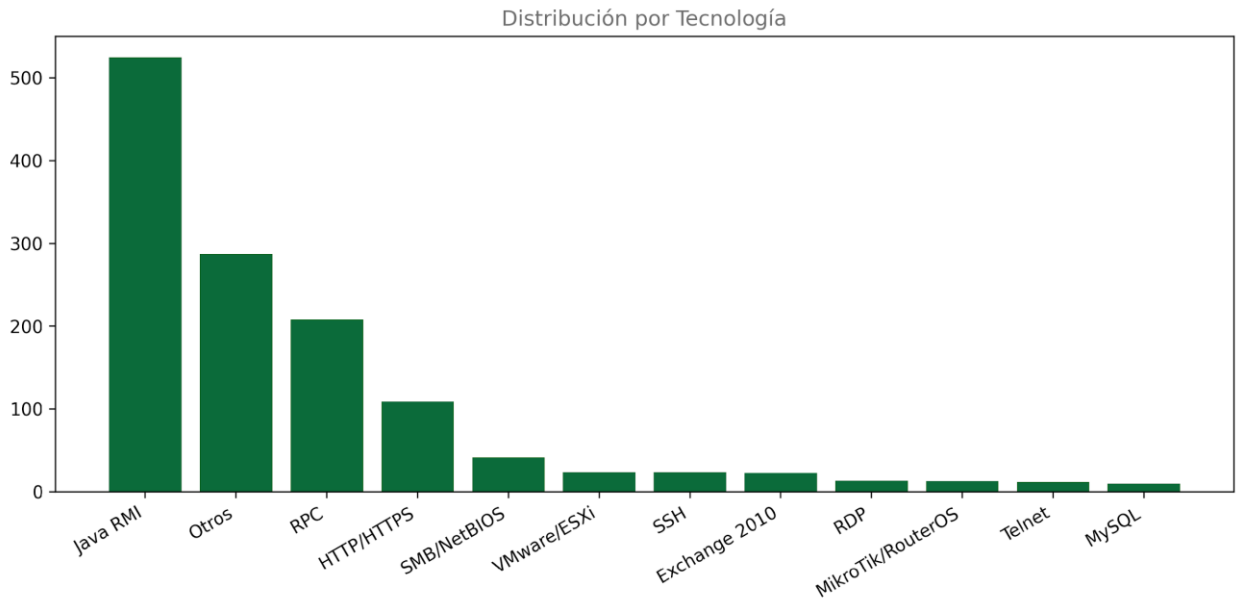
Cuadro comparativo de soluciones (resumen)

Dominio	Solución	Licencia	Capacidades	Pros	Contras	Recomendación	Prioridad
EDR	Opción A (existente): WithSecure	Comercial	Prevención+detección+respuesta	Integrado ya; soporte	Costo licenciamiento	Mantener y ampliar a 100%	Alta
SIEM	Opción A: Wazuh	Open Source	SIEM/NIDS/FIM/Agentes	Sin licencias; flexible	Curva operativa/infra	Piloto + sizing + runbook	Alta
SIEM	Opción B: Microsoft Sentinel	Comercial/Cloud	Escalable; reglas/ML	Tiempo-valor rápido	Costo por ingestión	POC 30 días y estimación OPEX	Alta
WAF	Opción A: Nginx+ModSecurity/OWASP CRS	Open Source	Protección capa 7	Costo bajo	Tuning y mantenimiento	Implementar en portales	Media

WAF	Opción B: Cloud WAF (Akamai/Cloudflare)	Comercial	Gestión sencilla global	Baja operación	Costo mensual	POC en servicios externos	Media
PAM	Opción A: Teleport/HashiCorp Boundary	Open Source	Acceso privilegiado seguro	OSS; auditable	Complejidad inicial	Piloto para admins	Media
PAM	Opción B: CyberArk/Delinea	Comercial	PAM maduro enterprise	Funcionalidad completa	Licenciamiento	Evaluar para criticidad	Media

11. KPIs y Roadmap

- KPIs: % Alta ≤90d (meta ≥90%), MTTR por severidad, cobertura EDR críticas (100%), % activos parcheados ≤180d (≥95%), % apps críticas con WAF/DAST, % servicios con MFA.



12. Integración de planes y anexos

- Excel/Dashboard: checklist_acciones.xlsx
- Plan de Ciberseguridad (ISO 27032)
- Plan de Continuidad Operativo (ISO 22301)

CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCION
18/09/2025	0	Versión inicial, Modelo de Seguridad y Privacidad de la Información

Elaboró	**Revisó**	**Aprobó**
Mauricio Rodríguez García Katherinne Silva Garibello	Mesa Temática	Comité Institucional de Gestión y Desempeño
Oficina Asesora de Direccionamiento Estratégico TIC	Jefe Oficina Planeación Institucional y Direccionamiento Estratégico	Dirección General
10/08/2025	11/09/2025	18/09/2025