Agencia Nacional de Minería

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2025

Omar Tique
Especialista en Seguridad de la información
Luis Alonso Lugo Charry
Oficial de seguridad de la información
CISO

Diciembre 29 de 2024

Contenido

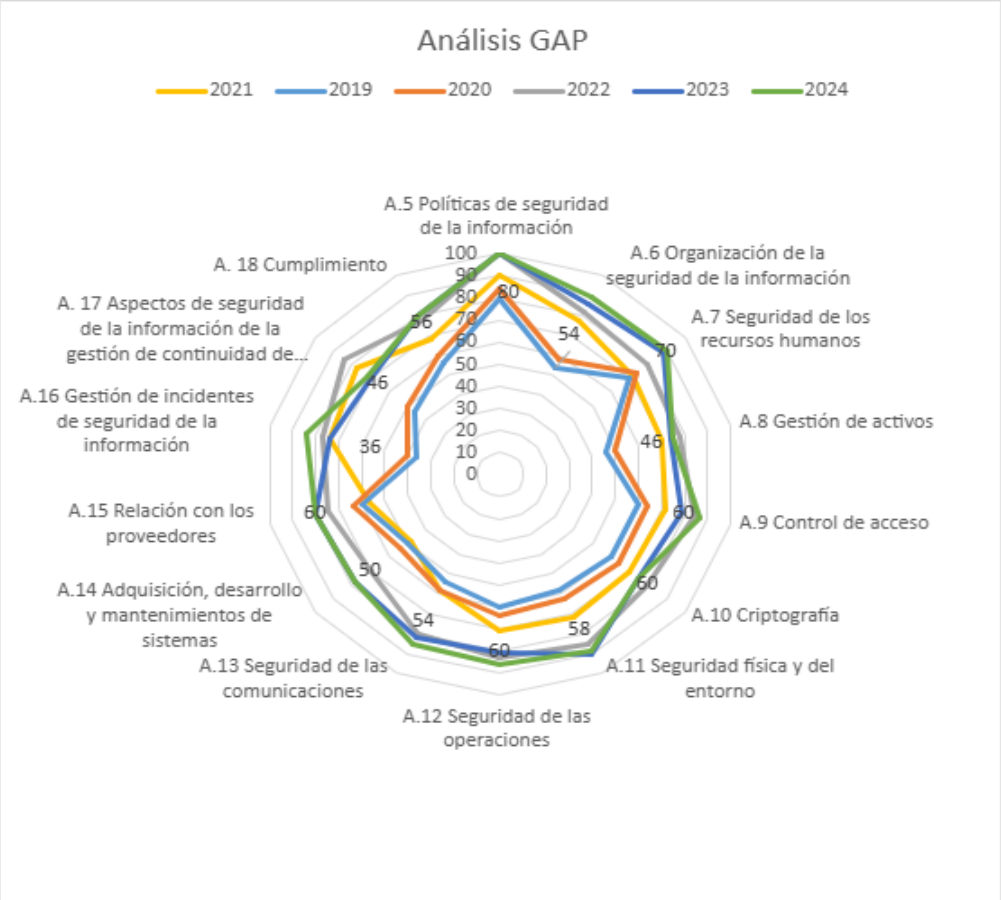
1. INTRODUCCIÓN y OBJETIVOS

Este informe establece el plan estratégico a desarrollar en el año 2025, con base en el avance realizado en el año 2024. Se encuentra alineado con el plan estratégico de tecnologías de información PETIC, con el plan de arquitectura empresarial en su dominio de seguridad y con la política de gobierno y seguridad digital del estado colombiano.

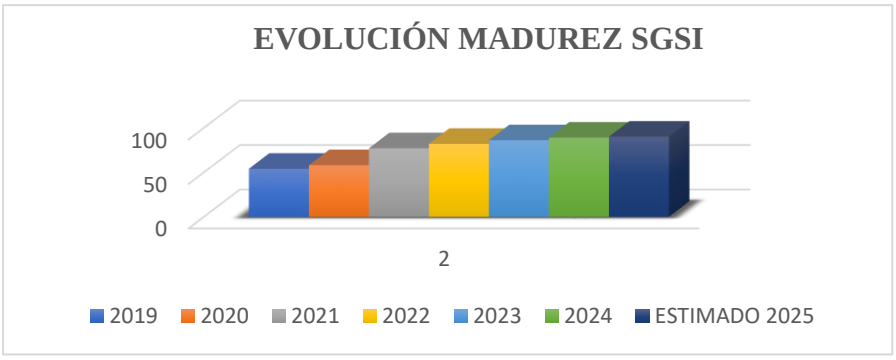
Con el alcance logrado en la vigencia 2024 estima mostrar un panorama para el año 2025 haciendo uso de los recursos disponibles y un planteamiento de necesidades de recursos de inversión para el año 2025.

2. Modelo de la Seguridad y Privacidad de la Información

El siguiente análisis GAP establece la evolución por años de los controles asociados al SGSI.



Fuente: Imagen original de la ANM- Matriz SOA



Fuente: Imagen original de la ANM

3. RESULTADO DEL AÑO 2024

Para el año 2024, se estimó un avance y refinamiento de los controles para llegar al 83% de madurez. Realizando una evolución estimada en cada uno de los siguientes dominios.

DOMINIO	2023	1° Semestre 2024	2° Semestre 2024
A.5 Políticas de seguridad de la información	**100**	**100**	**100**
A.6 Organización de la seguridad de la información	**86**	**89**	**89**
A.7 Seguridad de los recursos humanos	**89**	**90**	**90**
A.8 Gestión de activos	**74**	**73**	**75**
A.9 Control de acceso	**79**	**82**	**87**
A.10 Criptografía	**75**	**75**	**75**
A.11 Seguridad física y del entorno	**90**	**83**	**89**
A.12 Seguridad de las operaciones	**81**	**84**	**86**
A.13 Seguridad de las comunicaciones	**82**	**85**	**85**
A.14 Adquisición, desarrollo y mantenimientos de sistemas	**78**	**78**	**78**
A.15 Relación con los proveedores	**80**	**80**	**80**
A.16 Gestión de incidentes de seguridad de la información	**74**	**76**	**84**
A. 17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	**70**	**70**	**72**
A. 18 Cumplimiento	**80**	**80**	**80**
Promedio evaluación de controles	**81**	**82**	**83,6**

Durante la vigencia 2024 se realizaron actividades encaminadas a mejorar y mantener la postura de seguridad de la información de la ANM, las más relevantes fueron:

1. Actualización al manual de políticas de seguridad de la información.
2. Actualización, implementación, capacitación y seguimiento al procedimiento de gestión de incidentes de seguridad de la información.
3. Fortalecimiento en los controles de MS 365 relacionados con Fuga de información.
4. Fortalecimiento de la seguridad perimetral con enfoque en aplicaciones con el cierre de protocolos inseguros en los dispositivos de seguridad.

5. Cumplimiento del 75% del plan de trabajo de aseguramiento de Redes.
6. Revisión Y Auditoría interna de controles del SGSI especialmente en dominios de Control de acceso, seguridad física.
7. Fortalecimiento de los seguimientos a las copias de seguridad como fuente principal de un plan de recuperación de desastres.

4. PROYECCION 2025

Teniendo en cuenta el resultado de la vigencia 2024 y que los siguientes dominios no alcanzaron la meta del periodo, se estima importante en la vigencia 2025 dar prioridad al refuerzo de los dominios posteriormente resaltados:

DOMINIO	ESTIMADO 2024	EJECUTADO 2024	ESTIMADO 2025
A.5 Políticas de seguridad de la información	100	**100**	**100**
A.6 Organización de la seguridad de la información	87	**89**	**90**
A.7 Seguridad de los recursos humanos	89	**90**	**90**
A.8 Gestión de activos	80	**75**	**80**
A.9 Control de acceso	83	**87**	**90**
A.10 Criptografía	77	**75**	**80**
A.11 Seguridad física y del entorno	85	**89**	**90**
A.12 Seguridad de las operaciones	83	**86**	**88**
A.13 Seguridad de las comunicaciones	82	**85**	**86**
A.14 Adquisición, desarrollo y mantenimientos de sistemas	80	**78**	**80**
A.15 Relación con los proveedores	82	**80**	**85**
A.16 Gestión de incidentes de seguridad de la información	80	**84**	**85**
A. 17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	80	**72**	**80**
A. 18 Cumplimiento	80	**80**	**85**
Promedio evaluación de controles	**83,4**	**83,6**	**86,4**

5. REFUERZO DE CONTROLES PARA LLEGAR AL 86,4% DE CUMPLIMIENTO EN MATRIZ SOA:

ÍTEM DOMINIO	CONTROL	DESCRIPCIÓN CONTROL/OBJETIVO
A.6.1.3	Contacto con las autoridades	Se deben mantener los contactos apropiados con las autoridades pertinentes. Se debe realizar un listado de los contactos con autoridades y proveedores para colocarlos en un listado compartido
A.6.1.4	Contacto con grupos de interés especial	Se debería mantener los contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.2.1	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. Se debe realizar la restricción de la conexión a servicios de información, a los dispositivos móviles para aquellos usuarios que no cuenten con la autorización del jefe inmediato. Para los dispositivos móviles corporativos se deberían controlar con una solución MDM. (Mobile Device Management, solución que permite gestionar, controlar y proteger los datos corporativos de los dispositivos móviles celulares).
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deberían tener un propietario. Dar continuidad a la labor de inventario de Activos de información
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. Se debe establecer los controles de verificación de activos de información
A.8.2.2	Etiquetado de la información	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. Se debe implementar las acciones para la clasificación de los Activos,

ÍTEM DOMINIO	CONTROL	DESCRIPCIÓN CONTROL/OBJETIVO
A.8.3.2	Disposición de los medios	Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.9.2.1	Registro y cancelación del registro de usuarios	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. Establecer la identificación de los roles y perfiles desde los sistemas de información críticos para la entidad. Se debe implementar gestión de usuarios a nivel de aplicaciones
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado. Se debe implementar y controlar acceso privilegiados por Ciberark
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro. Se debe hacer una revisión y mejora en políticas de red
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.5	Control de acceso a códigos fuente de programas	Se debería restringir el acceso a los códigos fuente de los programas.
A.10.1.1	Política sobre el uso de controles criptográficos	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida. Se debe llevar controles de habilitación y des habilitación de llaves criptográficas.
A.12.1.3	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.

ÍTEM DOMINIO	CONTROL	DESCRIPCIÓN CONTROL/OBJETIVO
A.12.3.1	Respaldo de información	Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. Se debe establecer un plan de copias para SGD y la infraestructura de ORACLE.
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. Se debe realizar nuevamente escaneo y plan de remediación de vulnerabilidades
A.13.1.1	Controles de redes	Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes. Plan de trabajo con el profesional de redes para validar políticas de seguridad sobre las VLAN
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas. Implementar controles de doble factor de autenticación para el acceso a los sistemas de información y aplicativos webs de la ANM. Se tiene más de un 80% del MFA habilitado para Office 365
A.14.2.1	Política de desarrollo seguro	Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los

ÍTEM DOMINIO	CONTROL	DESCRIPCIÓN CONTROL/OBJETIVO
		desarrollos que se dan dentro de la organización.
A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. Se debe realizar las acciones para establecer la contingencia en la infraestructura de ORACLE
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. Programar las pruebas de continuidad a la plataforma crítica
A.18.1.3	Protección de registros	Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de

ÍTEM DOMINIO	CONTROL	DESCRIPCIÓN CONTROL/OBJETIVO
		acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.5	Reglamentación de controles criptográficos	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. Implementación de Cifrado de información en Reposo
A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información. Se deben realizar validaciones a los principales controles de cumplimiento técnico.

6. MIGRACION DE VERSION ISO 27001:2013 A ISO 27001:2022

Dentro de los objetivos estratégicos de la entidad se encuentra la certificación en la norma ISO27001. La ANM desde el año 2021 ha empezado a implementar el SGSI basado en la versión 2013 de la norma. Sin embargo, a partir del 1ro de mayo de 2024 el organismo rector de la norma ISO/IEC estableció que todas las entidades deben certificarse en las nuevas versiones bajo el modelo 2022.

Basado en lo anterior en la vigencia 2024 se realizó la contratación de un diagnóstico y un análisis de brecha entre las dos versiones de la norma, motivo por el cual en la vigencia 2025 se debe establecer un plan de adecuación de los controles y los requisitos de la nueva versión 2022.

7. GESTION DOCUMENTAL VIGENCIA 2025

Conforme el plan de reingeniería realizado en la vigencia 2024 y con base en los requisitos documentales de los diferentes organismos externos como son:

- MINTIC – Función pública, Política de gobierno digital – política de seguridad digital del Estado colombiano.
- Gestión documental ANM – Tablas de retención documental ANM.
- Clasificación de Activos de información – Ley 1712 de 2014.
- Modelo de Seguridad y Privacidad de la Información – MSPI
- Norma ISO27001:2022

- Modelo Guía de implementación de controles ISO27002:2022

Para el año 2025 se estima importante dar continuidad a la realización de documentos que respalden la gestión del SGSI, Por lo anterior, a nivel documental se estima presentar documentación necesaria y faltante que nos lleve al cumplimiento de ese 86.4% de avance en la matriz SOA, tales como:

1. Gestión de Activos de información, etiquetado, clasificación, actualización de catálogo. Etc.
2. Gestión de los medios removibles y borrado seguro de información
3. Proceso formal de registro y de cancelación de registro de usuarios y revocación de derechos. (incluye aplicaciones) y revisiones periódicas de los mismos.
4. Formalizar el nivel de acceso a aplicaciones.
5. Documentación de separación de ambientes en proyectos de implementación, pruebas y desarrollo.
6. Procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
7. Procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados
8. Procedimiento de desarrollo de sistemas y ciclo de vida.
9. Instructivo de manejo de contraseñas para administradores

8. PLAN DE CAPACITACIÓN Y CONCIENCIACIÓN

Se continuará con los planes de capacitación bajo la misma metodología con la que hemos venido haciéndolo en el año 2024 generando entre 6 y 10 capacitaciones generales en seguridad de la información y las capacitaciones específicas que sean requeridas por las diferentes áreas de la entidad.

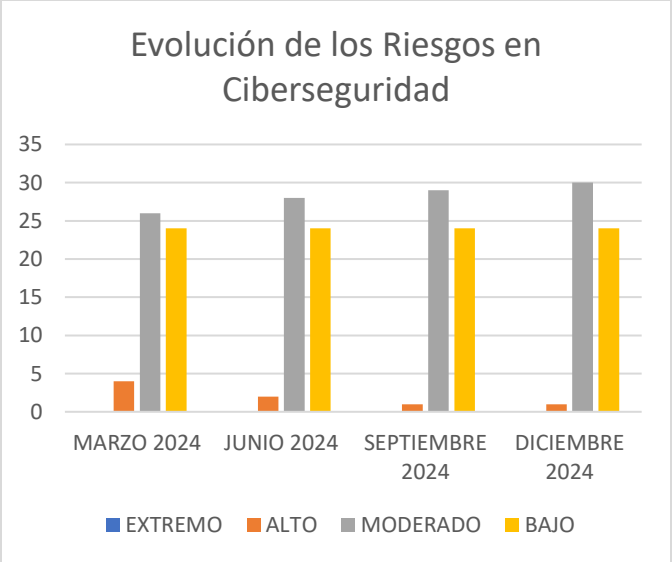
Se apoyará la concienciación con entidades externas a la Agencia Nacional de Minería como lo es con el ColCERT (CSIRT) Gobierno.

9. GESTIÓN DE RIESGOS DE SEGURIDAD

El informe detallado de la evolución de los riesgos durante la vigencia 2024, se puede encontrar en los informes de TRATAMIENTO DE RIESGOS 2024 (información de carácter público reservado)

NIVEL	DIC 2023	MARZO 2024	JUNIO 2024	SEPTIEMBRE 2024	DICIEMBRE 2024
EXTREMO	1	0	0	0	0
ALTO	3	4	2	1	1
MODERADO	39	26	28	29	30
BAJO	11	24	24	24	24
TOTAL	54	54	54	54	55

Fuente. Matriz de Riesgos en Ciberseguridad



Fuente. Matriz de Riesgos en Ciberseguridad

9.1. Estado de los Riesgos a finalizar el periodo 2024:

9.2. Proyección de la gestión de riesgos en el periodo 2025

1. El plan de mitigación de riesgos debe enfocarse en la infraestructura ORACLE que actualmente no posee planes de alta disponibilidad, a la actualización de las versiones mitigando posibles vulnerabilidades en los sistemas operativos.

2. Se debe dar continuidad al plan de seguridad de la plataforma 365, en especial a las relacionadas con fuga de información, pero también al uso de herramientas como Azure active Directory, Intune, y el componente EMS E3, que permita mitigar los riesgos en perdida de confidencialidad.

3. Se debe seguir incrementando los controles sobre conexiones remotas, en especial las generadas a través de VPN, tales como la implementación de un NAC (Network Acces Control), endurecimiento de control de antivirus en equipos no corporativos (de teletrabajo y contratistas), VPN cero confianzas, Auditoria de cumplimiento de equipos de cómputo de terceros.

4. Incrementar los mecanismos y procedimientos de Borrado Seguro y de cifrado de datos en reposo.

5. Mantener el plan de contrataciones en especial con proveedores y contratistas críticos para la continuidad de los servicios de la OTI. Así como la gestión temprana de procesos de contratación.

6. Realizar la contratación de personal enfocado en la mitigación de vulnerabilidades técnicas sobre infraestructura y bases de datos.

7. Dar continuidad y mantenimiento al tratamiento y gestión de los riesgos MODERADOS, estableciendo controles alternos y poder realizar la recalificación en nivel BAJO.

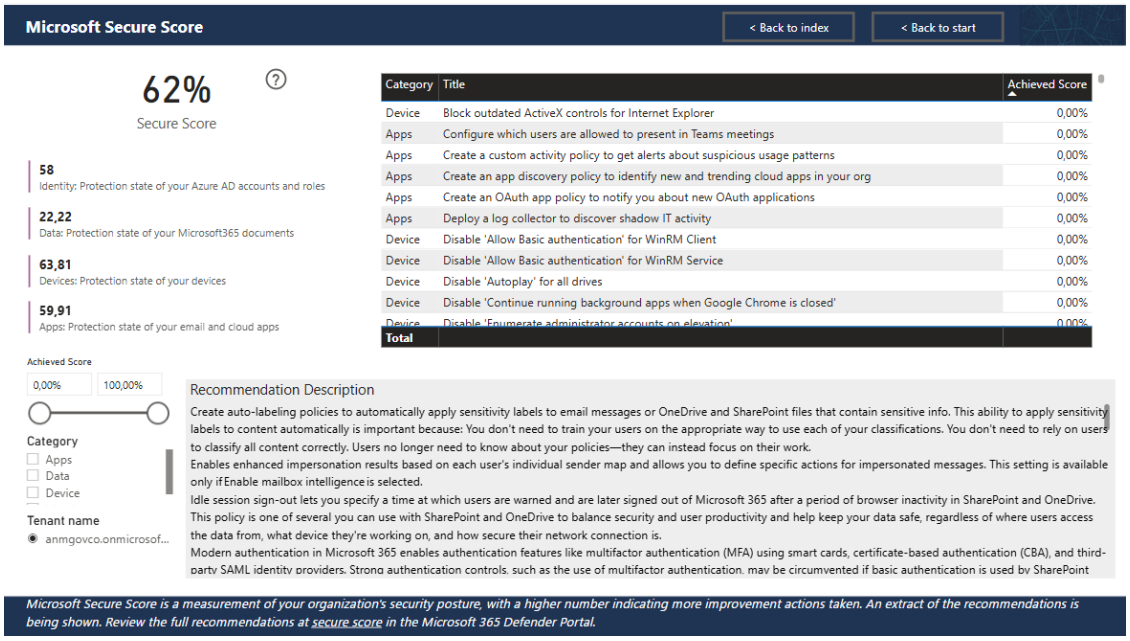
10. Gestión de Vulnerabilidades Técnicas

10.1. Gestión de Vulnerabilidades Microsoft 365

Como resultado del plan de trabajo ejecutado en el año 2024.se obtuvo un nivel de seguridad correspondiente al 62% de efectividad conforme el resultado de la prueba CSAT generada por el proveedor MICROSOFT; Las pruebas realizadas sobre la infraestructura evaluada, es posible concluir que existe un nivel de exposición Critico del 17,2% del total de vulnerabilidades Por ende el plan de trabajo del año 2025 se centrará en la mitigación de dichas vulnerabilidades con Actividades como:

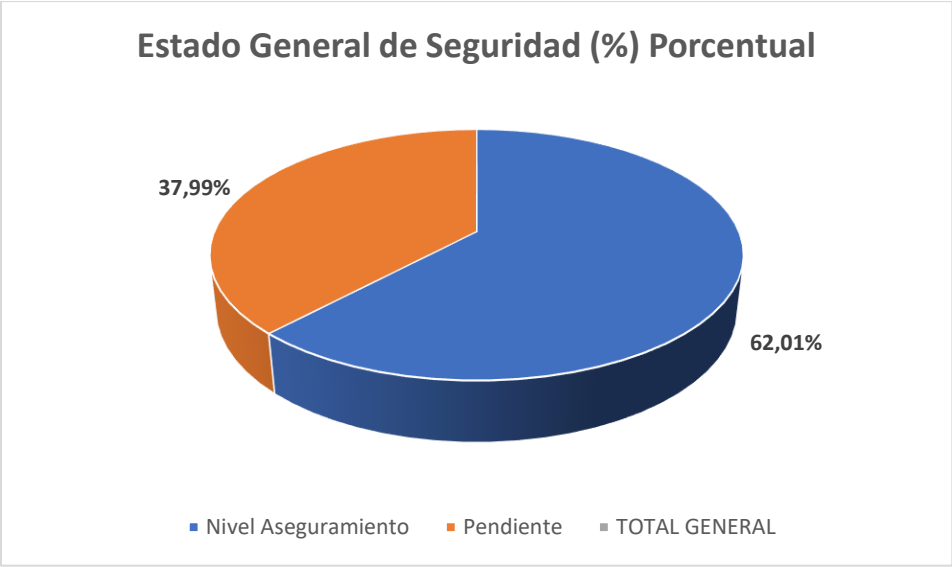
1. Control de dispositivos.
2. Clasificación de la información confidencial (en términos de ley 1712 Clasificada y reservada)
3. Control de fugas de información
4. Cifrado de la información en dispositivos móviles.
5. Gestión de vulnerabilidades en servidores Microsoft.
6. Habilitación del BitLocker en los End Points para el cifrado de la información en reposo.

Nivel de aseguramiento de la plataforma y productos Microsoft



Fuente. Interfaz herramienta Cloud Security Assessment Tools CSAT Microsoft, diciembre 2024.

El siguiente análisis refiere el nivel de aseguramiento de los servicios y plataformas de Microsoft con los cuales cuenta la Agencia Nacional de Minería para la vigencia de 2024, sin embargo, es de tenerse en cuenta que en este análisis se ha evaluado el estado de los sistemas operativos y en especial aquel que se encuentra en los End Points y que usa el sistema operativo de Windows 10, el cual tiene vigencia de soporte hasta el 14 de octubre de 2025.



Fuente. Análisis de resultado mediante Excel, Omar Tique M., diciembre 2024.

CATEGORY	PUNTUACIÓN	%
Nivel Aseguramiento	**204**	**62,01**
Pendiente	**125**	**37,99**
TOTAL, GENERAL	**329**	**100,0%**

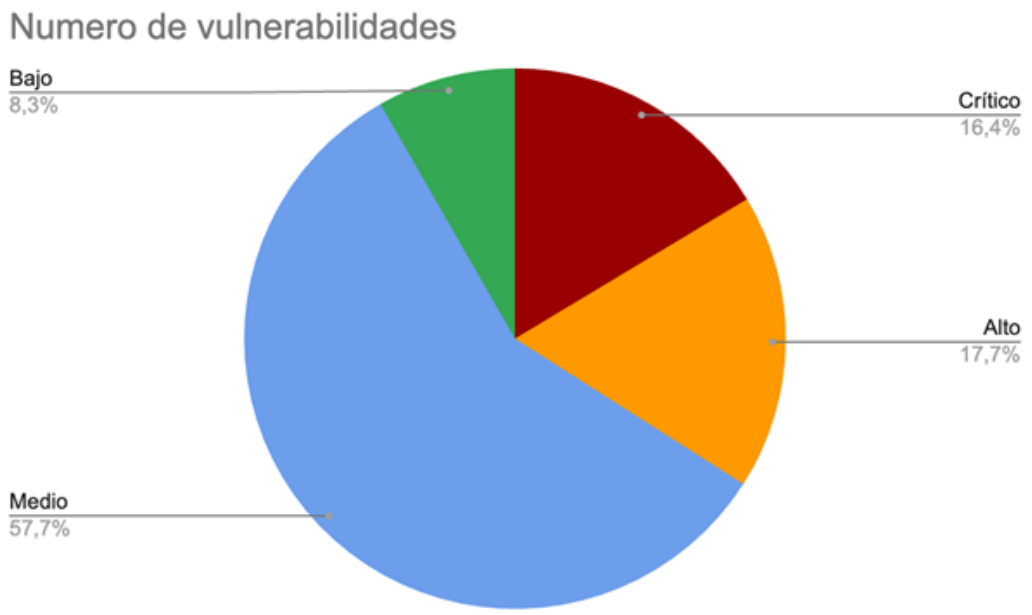
Fuente. Análisis de resultado mediante Excel, Omar Tique M., diciembre 2024.

10.2. Gestión de Vulnerabilidades internas

De acuerdo con el análisis de parte externa contratado para la vigencia 2024. Y los cuales han sido ejecutados de la siguiente forma, uno inicial principal y el segundo que corresponden al realizado una vez han sido realizadas las actividades de remediación y el cual se denomina (Retest), el cual fue ejecutado finalizando el segundo semestre.

Durante el año 2024 los diferentes profesionales se centraron en mitigar las vulnerabilidades críticas realizadas en el primer trimestre de 2024. Al finalizar el segundo semestre de 2024 el resultado fue el siguiente:

- Se cerraron 119 vulnerabilidades de 3333 halladas en la ejecución del primer Pentest de las cuales 19 son críticas.
- Se remediaron de igual forma 127 vulnerabilidades que fueron hallada en un total de 13 direcciones IP´s.
- Finalmente se conservan 3102 vulnerabilidades de las 3333 vulnerabilidades halladas en las pruebas inicialmente ejecutadas.
- Sin embargo, en la prueba de Retest, se han hallado 856 vulnerabilidades nuevas en un total de 237 activos en el periodo comprendido de junio a diciembre 2024.



Fuente. Análisis de resultado agente externo, Retest, Omar Tique M., diciembre 2024.

RIESGO	N°. VULNERABILIDADES	%
Crítico	**647**	**16,37**
Alto	**698**	**17,66**
Medio	**2280**	**57,69**
Bajo	**327**	**8,27**
TOTAL	**3952**	**100,00**

Fuente. Análisis de resultado agente externo, Retest,
Omar Tique M., diciembre 2024.

10.3. Proyección de la gestión de vulnerabilidades en el periodo 2025

- Con base en las anteriores estadísticas, se observa la necesidad prioritaria de gestionar las vulnerabilidades de riesgo ALTO y EXTREMO a nivel de infraestructura.

- Se debe gestionar los recursos y el personal necesario para atender la remediación de las vulnerabilidades y en equipo con responsables y encargados de la operación actual realizar los procesos de ejecución de remediación.

- Es claro, que el alto volumen de trabajo en tan poco personal, especialmente en los encargados de infraestructura impacta el plan de trabajo de este proceso, situación que se ha expuesto ante la Dirección de la oficina de TI en varias oportunidades presentándose un riesgo importante de segmentación y segregación de funciones.

- En función de lo anterior, se recomienda darle la prioridad necesaria por parte de la dirección de la oficina de Tecnologías e información asignado las directrices, los recursos humanos, el presupuesto y herramientas necesarias, así como la priorización en los cronogramas de trabajo y entregables en equipos responsables.

- El fortalecimiento del equipo de infraestructura es un paso necesario ya que sobre este recae el 90% de la ejecución de este plan.

- Darle la importancia que requiere, es inminente ante los constantes ataques informáticos donde el canal más explotado en la ciberdelincuencia corresponde justamente al aprovechamiento de debilidades en los sistemas para el robo y/o secuestro de información o la indisponibilidad de los sistemas afectando la integridad, la confidencialidad de la información o en su defecto la disponibilidad de los servicios.

11. Gestión de la continuidad de Negocio

a. La OTI fue designada como la encargada de establecer el PLAN DE CONTINUIDAD DE NEGOCIO (BCP), se sugiero respetuosamente que esta designación sea revisada a nivel directivo ya que esta delegación debe estar en un área transversal de la Entidad como Planeación.

b. La Agencia Nacional de Minería implementó un proyecto de hyperconvergecia desde el año 2021 y como resultado de ese ejercicio para las plataformas críticas ANNA Minería, Portal Web, Control a la Producción, WEBSAFI y RUCOM se mantienen bajo esta arquitectura de continuidad del servicio tecnológico o PRD.

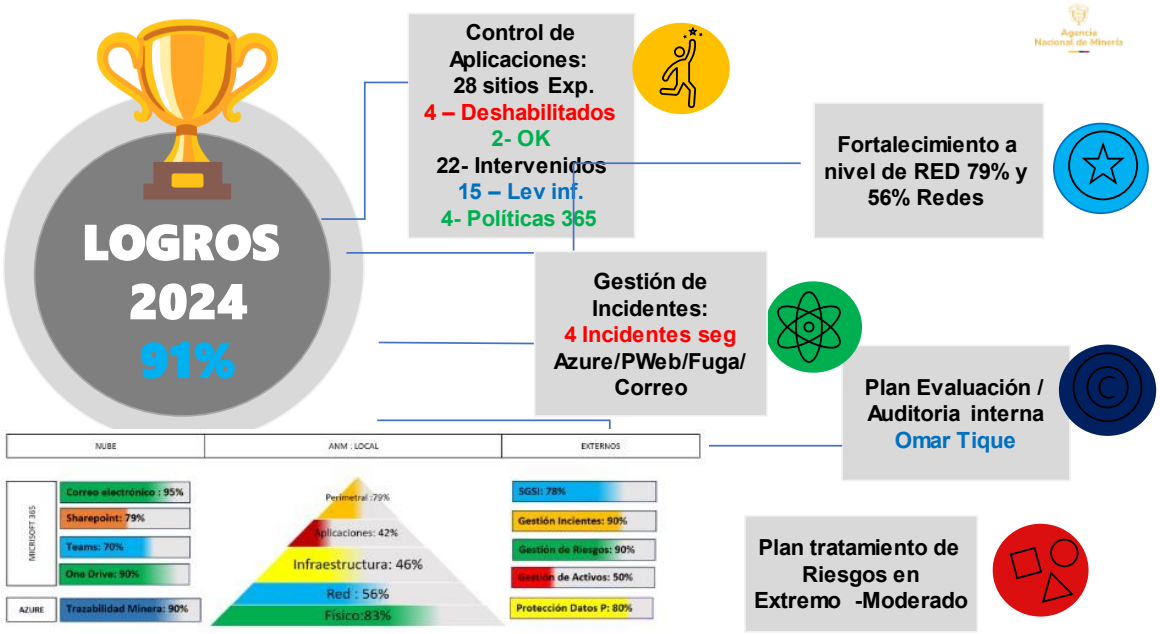
c. Para los sistemas de información o plataforma tecnológica que no quedarán soportados por estos nodos de hiperconvergencia se mantiene un esquema de copias de seguridad monitoreado, con seguimiento y validación de su generación y resultado.

d. La ANM cuenta con una infraestructura sobre ORACLE donde se soporta el SGD. Esta infraestructura desde el año 2023 se ha ampliado los

recursos tecnológicos para su funcionamiento. Durante el año 2025 se estima fortalecer la estructura de convergencia de esta plataforma.

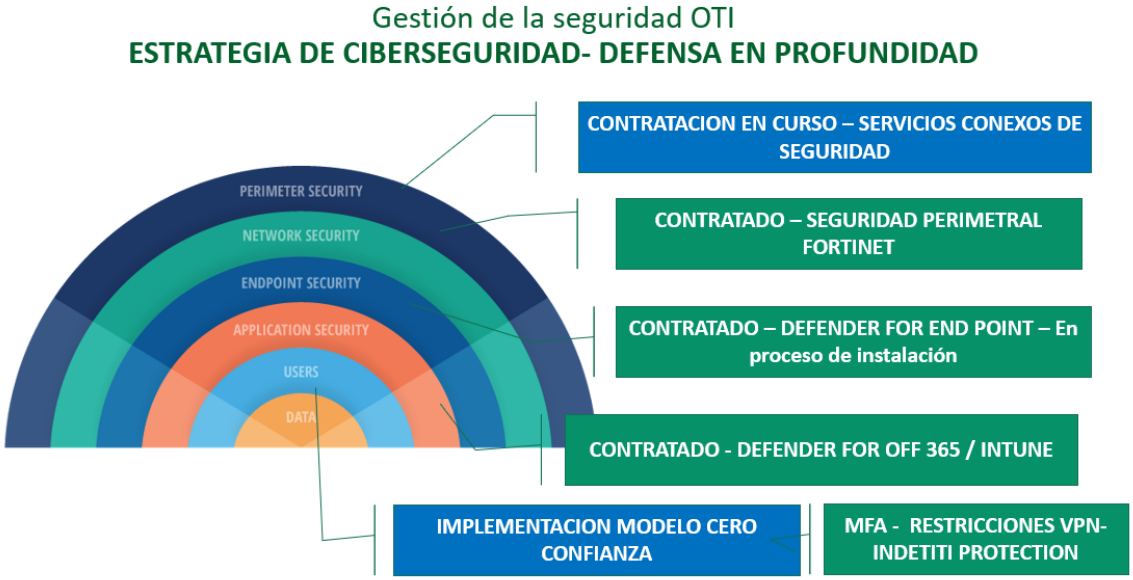
e. Durante la vigencia 2025 como parte del proceso de mejora continua se considera realizar auditoría interna y pruebas de funcionamiento al actual Plan de Recuperación de Desastres. Así mismo, resaltar la importancia al Comité de Gestión y desempeño de gestionar un Plan de Continuidad de Negocio.
f. la disponibilidad e integridad de la información y los datos.

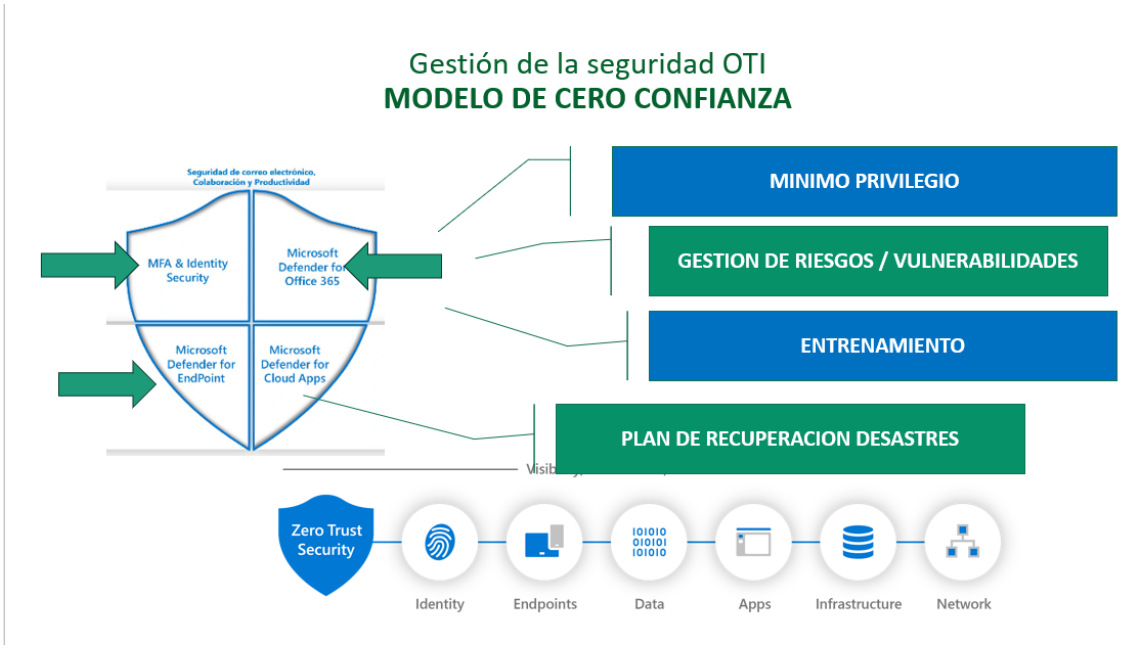
12. CONTINUIDAD DE LA ESTRATEGIA DE CIBERSEGURIDAD



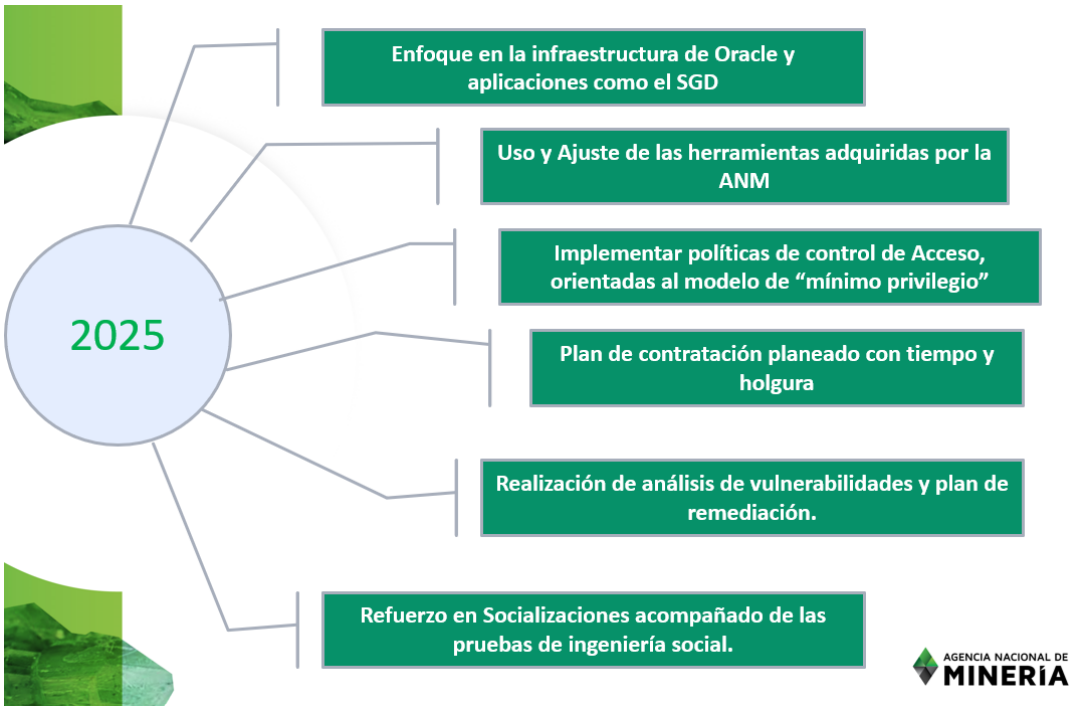
- Se dará continuidad a las medidas de seguridad a nivel de la plataforma 365 optimizando el componente EMS E3 adquirido por la entidad.

- Se debe dar continuidad a la implementación del esquema de defensa en profundidad manteniendo un enfoque de cero confianza y mínimo privilegio.





- Realizar una verificación de cumplimiento de los requisitos de seguridad de la información con los proveedores críticos.
- Enfoque de actividades relacionadas con el cumplimiento de controles del SGSI y Gobierno Digital.



Informe Realizado por Luis Alonso Lugo Charry – Oficial de seguridad de la información CISO

Agencia
Nacional de Minería