# Plan estratégico de Seguridad de la Información

# 2024

Luis Alonso Lugo Charry – Oficial de seguridad de la información CISO

Versión 1: diciembre 29 de 2023

## Contenido

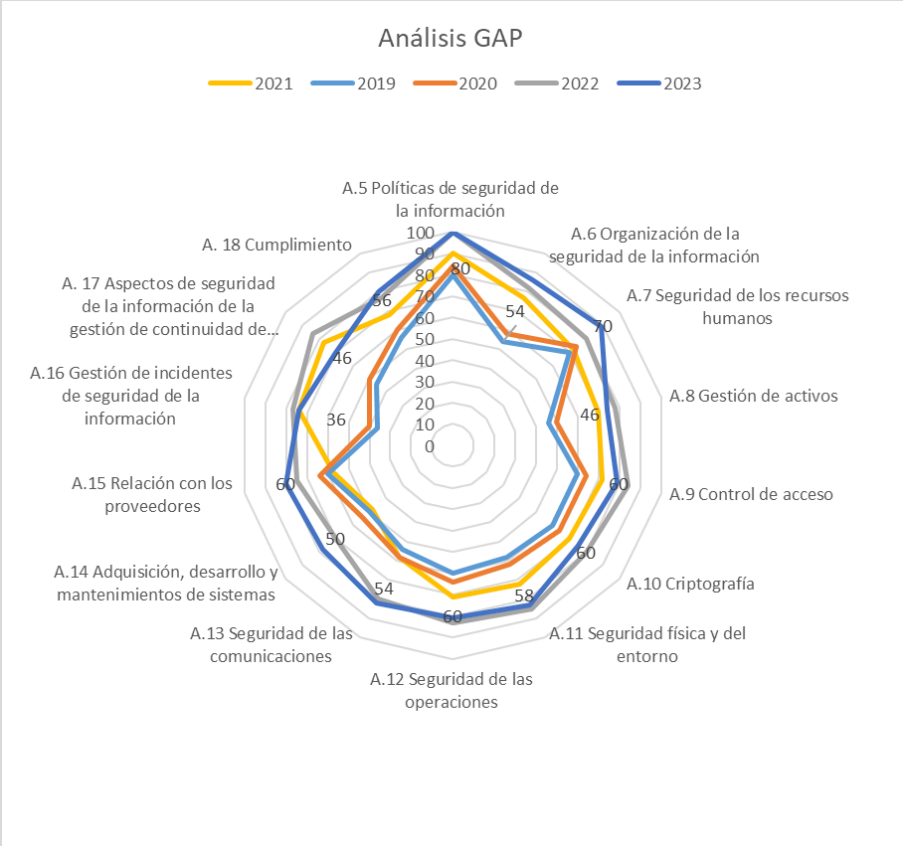
# 1. INTRODUCCIÓN y OBJETIVOS

Este informe establece el plan estratégico a desarrollar en el año 2024 , con base en el avance realizado en el año 2023, y que se encuentra alineado con el plan estratégico de tecnologías de información PETIC.

Estima mostrar un panorama de la proyección que se debe tomar, de los recursos disponibles y un planteamiento real con los recursos asociados

# 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

## 3. EVOLUCION DEL AÑO 2023

Para el año 2023, 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 | DIC 2022 | 2023 | EVALUACIÓN CUALITATIVA DE CONTROL |
|---|---|---|---|
| A.5 Políticas de seguridad de la información | 100 | 100 | **Optimizado** |
| A.6 Organización de la seguridad de la información | 82 | 85 | **Gestionado** |
| A.7 Seguridad de los recursos humanos | 80 | 85 | **Gestionado** |
| A.8 Gestión de activos | 78 | 85 | **Gestionado** |
| A.9 Control de acceso | 84 | 85 | **Gestionado** |
| A.10 Criptografía | 80 | 80 | **Gestionado** |
| A.11 Seguridad física y del entorno | 85 | 90 | **Gestionado** |
| A.12 Seguridad de las operaciones | 83 | 85 | **Gestionado** |
| A.13 Seguridad de las comunicaciones | 80 | 86 | **Gestionado** |
| A.14 Adquisición, desarrollo y mantenimientos de sistemas | 70 | 80 | **Efectivo** |
| A.15 Relación con los proveedores | 75 | 80 | **Gestionado** |
| A.16 Gestión de incidentes de seguridad de la información | 77 | 85 | **Gestionado** |

| | | | |
|---|---|---|---|
| A. 17 Aspectos de seguridad de la información de la gestión de continuidad de negocio | 84 | 84 | **Gestionado** |
| A. 18 Cumplimiento | 77 | 90 | **Optimizado** |
| **Promedio evaluación de controles** | **81** | **83** | **Gestionado** |

Tabla no 2. Proyección de controles del SGSI a cierre 2023

## 4. Evolución de Los controles por trimestre.

| DOMINIO | 2022 | 1ER TRIMESTRE 2023 | 2DO Trimestre 2023 | 3ER Trimestre 2023 | 4to Trimestre 2023 |
|---|---|---|---|---|---|
| A.5 Políticas de seguridad de la información | 100 | 100 | 100 | 100 | 100 |
| A.6 Organización de la seguridad de la información | 82 | 85 | 86 | 86 | 86 |
| A.7 Seguridad de los recursos humanos | 80 | 80 | 83 | 83 | 89 |
| A.8 Gestión de activos | 78 | 79 | 73 | 74 | 74 |
| A.9 Control de acceso | 84 | 85 | 81 | 81 | 81 |
| A.10 Criptografía | 80 | 80 | 80 | 80 | 80 |
| A.11 Seguridad física y del entorno | 85 | 84 | 81 | 81 | 83 |
| A.12 Seguridad de las operaciones | 83 | 76 | 68 | 70 | 81 |
| A.13 Seguridad de las comunicaciones | 80 | 79 | 68 | 68 | 82 |
| A.14 Adquisición, desarrollo y mantenimientos de sistemas | 70 | 70 | 70 | 72 | 78 |
| A.15 Relación con los proveedores | 75 | 76 | 69 | 74 | 80 |
| A.16 Gestión de incidentes de seguridad de la información | 77 | 71 | 51 | 53 | 74 |
| A. 17 Aspectos de seguridad de la información de la gestión de continuidad de negocio | 84 | 64 | 54 | 54 | 70 |
| A. 18 Cumplimiento | 77 | 77 | 74 | 74 | 80 |
| **Promedio evaluación de controles** | **81** | **79** | **74** | **75** | **81** |

Durante el periodo del 2023 se realizó seguimiento trimestral a los controles del SGSI por los constantes cambios en las modalidades de contratación de la ANM y el ingreso de la nueva administración.

Se observó que en el **1er Trimestre** se generó un impacto negativo tras el vencimiento de los servicios del SOC y las licencias de los dispositivos de seguridad, así como el vencimiento del contrato del profesional de redes y ciberseguridad, lo que nos obligó a establecer controles alternos tales como:

1. Implementación de un equipo de atención de incidentes con el recurso humano de la OTI, a través de socialización y capacitación del personal.
2. Revisión de los planes de contingencia, revisión de copias de seguridad, verificación de componentes de infraestructura contra incidentes.
3. Remediación de Vulnerabilidades críticas.
4. Se inicio con el plan de reconocimiento de Activos
5. Revisión y refuerzo de los controles de acceso en diferentes aplicaciones.
6. Control con proveedores para los accesos a los recursos de la entidad.

A pesar de las acciones tomadas nos definió en una calificación del 79% de cumplimiento. Es decir, una disminución de 2 puntos en la medición del trimestre inmediatamente anterior.

En el **segundo Trimestre se** dio por culminado el contrato de del End point McAfee lo que impacto de nuevo de manera negativa los controles asociados al manejo de la seguridad de red. Por consiguiente, se tomaron las siguientes acciones:

1. Priorización de acciones para la retoma de contratos
2. Priorizar la contratación del profesional de redes y ciberseguridad.
3. Refuerzo en las políticas de teletrabajo, orientado a establecer controles de conectividad remota.

Sin embargo, el vencimiento de dichos contratos nos afectó negativamente el nivel de madurez disminuyendo 5 puntos con relación al trimestre inmediatamente anterior.

En el **Tercer Trimestre el** enfoque se desarrolló en la recuperación de los servicios afectados por la contratación, recuperando en primera medida el contrato de licenciamiento de los sistemas Fortinet y retornar el control sobre redes y seguridad perimetral.

Lo anterior se evidencia en una leve recuperación de la calificación general, y un importante resultado en los dominios de comunicaciones, operaciones e incidentes.

Durante el **cuarto Trimestre** se recuperaron los contratos de Seguridad del End point, Se retomaron los contratos del SOC/SIEM y equipo de gestión de incidentes con la corporación RENATA, Se validaron la gestión del 95% de vulnerabilidades críticas y un 26% de las vulnerabilidades de categoría alta.

El impacto sobre la calificación fue notable en todos los dominios, recuperando el terreno perdido en los dos primeros trimestres.

Adicionalmente se adquirieron herramientas para el control de identidad a través del componente EMS E3 de Microsoft.

De igual manera tras la renovación de las licencias de los equipos de la seguridad perimetral, le dio vía al profesional de redes para proceder a las actualizaciones de las versiones vulnerables de los dispositivos de redes, la hardenización de políticas de seguridad y la aplicación de políticas de

navegación por el Web Proxy.

Por lo anterior la calificación al final del periodo se dio en un 81,11% superando en 011% la calificación de cierre del año 2022.

Desafortunadamente no se llegó a la meta estimada, aunque se creció levemente en la calificación general. Esta situación nos permitió reforzar en controles que teníamos en responsabilidad de terceros y que ahora están bajo el control del equipo de la OTI en la ANM.

Nuevamente la meta se establece en un 83,5% para el año 2024.

## 5. REFUERZO DE CONTROLES PARA LLEGAR AL 83,5% DE CUMPLIMIENTO EN MATRIZ SOA:

| | | |
|---|---|---|
| A.6.1.3 | Contacto con las autoridades | Se deben mantener los contactos apropiados con las autoridades pertinentes.<br>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.<br>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.<br>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.<br>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.<br>Se debe establecer las técnicas de borrado seguro y 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.<br>Se debe implementar las acciones para la clasificación de los Activos,<br>Se Realiza la compra de las licencias EMS E3, pendientes los procesos de implementación |
| 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.9.1.1 | Política de control de acceso | Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. |
| 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.<br>Establecer la identificación de los roles y perfiles desde los sistemas de información críticos para la entidad.<br>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.<br>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.<br>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.9.4.4 | Uso de programas utilitarios privilegiados | Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones. |
| 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.<br>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. |

| | | |
|---|---|---|
| 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.<br>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.<br><br>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.<br><br>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.<br>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 desarrollos que se dan dentro de la organización. |
| A.16.1.1 | Responsabilidad y procedimientos | Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.<br>Realizar las pruebas y actualizar el procedimiento de gestión de incidentes |
| 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.<br>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.<br>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 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.<br>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.<br>Se deben realizar validaciones a los principales controles de cumplimiento técnico. |

## 6. Gestión Documental

Para el año 2024 se estima importante dar continuidad a la realización de documentos que respalden la gestión del SGSI y de la seguridad de la información

Por lo anterior a nivel documental se estima presentar documentación necesaria y faltante que nos lleve al cumplimiento de ese 83% de avance en la matriz SOA, tales como:

1. Documentación relacionada con la seguridad en el trabajo remoto.
2. Gestión de Activos de información, etiquetado, clasificación, actualización de catálogo. Etc.
3. Gestión de los medios removibles y borrado seguro de información
4. Proceso formal de registro y de cancelación de registro de usuarios y revocación de derechos. (incluye aplicaciones) y revisiones periódicas de los mismos.
5. Formalizar el nivel de acceso a aplicaciones.

6. Documentación de separación de ambientes en proyectos de implementación, pruebas y desarrollo.
7. procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
8. 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
9. Procedimiento de desarrollo de sistemas.
10. Instructivo de manejo de contraseñas para administradores
11. Plan de recuperación de desastres.

## 7. 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 2023 generando 6 capacitaciones generales en seguridad de la información y las capacitaciones específicas que sean requeridas por las diferentes áreas de la entidad.

## 8. Gestión de Riesgos de Seguridad

Durante el año 2023 se trabajó en la mitigación de los riesgos de estado extremo y alto presentando la siguiente evolución.

### 8.1 Resultado previo del 1er Trimestre

Teniendo el informe de Riesgos al finalizar año 2022 donde el panorama de riesgos se incrementó notablemente con la culminación de los contratos de seguridad y licenciamientos Fortinet, durante el primer trimestre en cabeza de la jefe de la OTI, el enfoque fue establecido a la normalización de las operaciones y la recuperación del ambiente de ciberseguridad que proporcionaba la tercerización de servicios en ciberseguridad y el aporte en la medición de controles del SGSI.

GESTION DE RIESGOS EXTREMOS:

Durante el cuarto trimestre del año la OTI se ha enfocado en la gestión y tratamiento de los Riesgos críticos a través de la contratación de servicios y herramientas de alto impacto para la Entidad. Es Así como se ha restaurado la contratación de los servicios SOC / SIEM / GESTION DE INCIDENTES / PRUEBAS DE VULNERABILIDAD/ ADMINISTRACION CIBERARK con la contratación de la entidad RENATA. Adicionalmente se inició la implementación de DEFENDER FOR END POINT de Microsoft, contratación adjudicada previamente a la empresa CONTROLES EMPRESARIALES quien ganó dicha oferta.

La Divisiones de infraestructura y sistemas de información de la OTI reportan la gestión del 95% de las vulnerabilidades críticas, mientras a nivel directivo se dio priorización a contrataciones críticas para la continuidad de la operación tecnológica de la Entidad.

## 8.2. Estado de los Riesgos a finalizar 4to Trimestre:

| | |
|---|---|
| EXTREMO | 1 |
| ALTO | 3 |
| MODERADO | 39 |
| BAJO | 11 |
| | 54 |

| | |
|---|---|
| OTROS | 2 |
| TECNOLOGICOS | 16 |
| SEGURIDAD DE LA INFORMACION | 21 |
| CIBERSEGURIDAD | 15 |
| | 54 |


## 8.3. Evolución de Los Riesgos:

| NIVEL | DICIEMBRE 2022 | MARZO 2023 | JUNIO 2023 | SEPT 2023 | DIC 2023 |
|---|---|---|---|---|---|
| EXTREMO | 2 | 7 | 8 | 2 | 1 |
| ALTO | 8 | 4 | 4 | 7 | 3 |
| MODERADO | 27 | 31 | 32 | 34 | 39 |
| BAJO | 9 | 10 | 10 | 11 | 11 |
| TOTAL | 46 | 52 | 54 | 54 | 54 |

8.4. Proyección de la gestión de riesgos en el periodo 2024

I. El plan de mitigación de riesgos debe enfocarse en la infraestructura ORACLE que actualmente no posee planes de contingencia, remediación de vulnerabilidades y el estado de las copias de seguridad es deficiente a la necesidad, dado las limitaciones de almacenamiento.

II. Se debe dar continuidad al plan de seguridad de la plataforma 365, en especial a la implementación del end point, 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.

III. Se debe seguir incrementando los controles sobre conexiones remotas, en especial las generadas a través de VPN, tales como la implementación de un NAC (Networ9k Acces Control), endurecimiento de control de antivirus en equipos no corporativos (de teletrabajo y contratistas)

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

V. Mantener el plan de contrataciones en especial con proveedores y contratistas críticos para la continuidad.

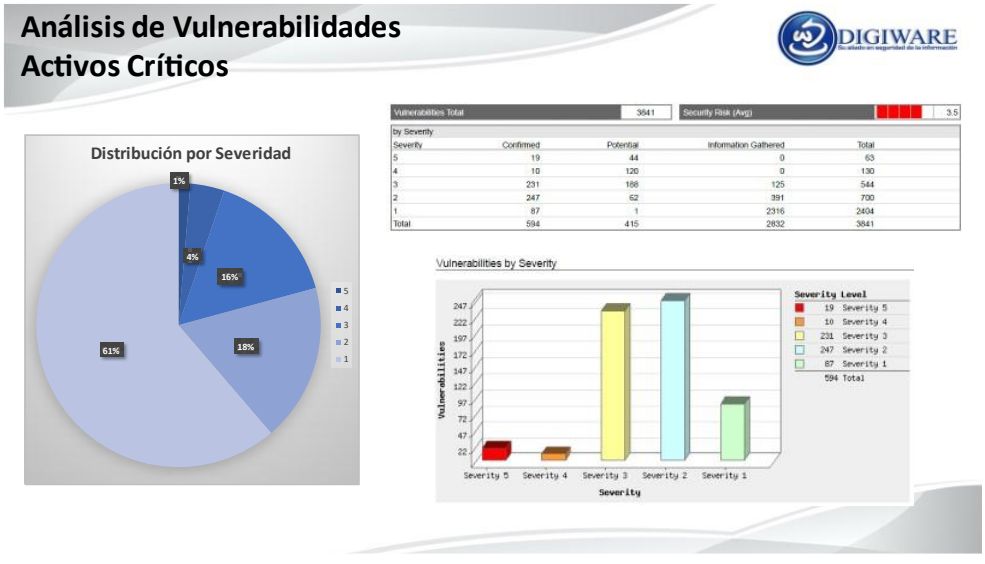
VI. Realizar la contratación de administradores de servicios Linux que apoyen la mitigación de vulnerabilidades en estos sistemas operativos.

## 9. Gestión de Vulnerabilidades Técnicas

Las vulnerabilidades técnicas que dependiendo de su clasificación corresponden a riesgos para la organización. No toda vulnerabilidad corresponde a una amenaza y por consiguiente no toda amenaza se convierte en riesgo

Durante el año 2023 fue incluido el análisis CISA. cuyo concepto corresponde a un estudio de las principales vulnerabilidades que están siendo a la fecha utilizada por los ciberdelincuentes.

Como resultado de las pruebas realizadas sobre la infraestructura evaluada, es posible concluir que existe un nivel de exposición Critico del 7% del total de vulnerabilidades. Mientras el 93% corresponde a nivel medio y bajo de exposición.



Con base del plan de trabajo realizado en el año 2023:

1. Se trabajaron cerca del 20% del total de las vulnerabilidades, pero que en función de priorizar el plan de trabajo en las vulnerabilidades Extremas y altas el resultado es el siguiente:
   - Se trataron cerca del 60% de las vulnerabilidades extremas y un 32% de las ALTAS.
   - Las vulnerabilidades que no se trataron corresponden a las de aplicaciones en Linux y a cargo del administrador de Linux, Rol que no fue contratado en el periodo 2023.
   - A la fecha se han trabajado cerca del 20% del total de las vulnerabilidades, pero que en función de priorizar el plan de trabajo en las vulnerabilidades Extremas y altas el resultado es el siguiente:
   - Se trataron cerca del 60% de las vulnerabilidades extremas y un 32% de las ALTAS.
   - Las vulnerabilidades que no se trataron corresponden a las de aplicaciones en Linux y a cargo del administrador de Linux, Rol que no fue contratado en el periodo 2023.

Distribución de las Vulnerabilidades por Gestionar:

| Etiquetas de fila | Cantidad | % |
|---|---|---|
| **Por Gestionar** | **1344** | **100,00%** |
| ALTO | 331 | 24,63% |
| BAJO | 401 | 29,84% |
| EXTREMO | 29 | 2,16% |
| MODERADO | 583 | 43,38% |
| **Total, general** | **1344** | **100,00%** |

| Etiquetas de fila | Cantidad | % |
|---|---|---|
| **Administrador Linux** | **79** | **5,88%** |
| **Por Gestionar** | **79** | **5,88%** |
| ALTO | 48 | 3,57% |
| EXTREMO | 7 | 0,52% |
| MODERADO | 24 | 1,79% |
| **Aleixandre Nick Tovar / Fabian Palomares** | **351** | **26,12%** |
| **Por Gestionar** | **351** | **26,12%** |
| BAJO | 300 | 22,32% |
| MODERADO | 51 | 3,79% |
| **Coordinador Mesa de Ayuda** | **3** | **0,22%** |
| **Por Gestionar** | **3** | **0,22%** |
| MODERADO | 3 | 0,22% |
| **Diego Leon / Fabian Palomares** | **15** | **1,12%** |

| | | |
|---|---|---|
| **Por Gestionar** | **15** | **1,12%** |
| MODERADO | 15 | 1,12% |
| **Diego Mojica** | **21** | **1,56%** |
| **Por Gestionar** | **21** | **1,56%** |
| ALTO | 14 | 1,04% |
| MODERADO | 7 | 0,52% |
| **Diego Mojica / Fabian Palomares** | **15** | **1,12%** |
| **Por Gestionar** | **15** | **1,12%** |
| ALTO | 8 | 0,60% |
| MODERADO | 7 | 0,52% |
| **Fabian Palomares** | **564** | **41,96%** |
| **Por Gestionar** | **564** | **41,96%** |
| ALTO | 212 | 15,77% |
| BAJO | 2 | 0,15% |
| MODERADO | 350 | 26,04% |
| **Fabian Palomares / Diego Mojica** | **7** | **0,52%** |
| **Por Gestionar** | **7** | **0,52%** |
| ALTO | 7 | 0,52% |
| **Fabian Palomares /Profesional de Redes** | **4** | **0,30%** |
| **Por Gestionar** | **4** | **0,30%** |
| MODERADO | 4 | 0,30% |
| **Fabian Palomares/ Administrador Linux** | **1** | **0,07%** |
| **Por Gestionar** | **1** | **0,07%** |
| MODERADO | 1 | 0,07% |
| **Felipe Andre Mouthon Sierra** | **3** | **0,22%** |
| **Por Gestionar** | **3** | **0,22%** |
| MODERADO | 3 | 0,22% |
| **Felipe Andre Mouthon Sierra / Administrador Linux** | **79** | **5,88%** |
| **Por Gestionar** | **79** | **5,88%** |
| ALTO | 35 | 2,60% |
| EXTREMO | 22 | 1,64% |
| MODERADO | 22 | 1,64% |
| **Jose Ricardo** | **22** | **1,64%** |
| **Por Gestionar** | **22** | **1,64%** |
| MODERADO | 22 | 1,64% |
| **Marcela Rubio** | **4** | **0,30%** |
| **Por Gestionar** | **4** | **0,30%** |
| ALTO | 4 | 0,30% |
| **Maria Isabel Gonzalez Buitrago / Fabian Palomares** | **154** | **11,46%** |
| **Por Gestionar** | **154** | **11,46%** |

| | | |
|---|---|---|
| BAJO | 99 | 7,37% |
| MODERADO | 55 | 4,09% |
| **Profesional de Redes** | **22** | **1,64%** |
| **Por Gestionar** | **22** | **1,64%** |
| ALTO | 3 | 0,22% |
| MODERADO | 19 | 1,41% |
| **Total, general** | **1344** | **100,00%** |

9.2. Proyección de la gestión de vulnerabilidades en el periodo 2024

- Con base en las anteriores estadísticas, se observa la necesidad prioritaria de gestionar las vulnerabilidades de riesgo ALTO y EXTREMO en servidores LINUX.
- 
- 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.
- 
- Teniendo en cuenta que los planes de trabajo se realizaron en el año 2022 y sobre este reporte se realizó el plan de trabajo de 2023, se estima conveniente la realización de un nuevo análisis de vulnerabilidades y un nuevo estudio de Ethical Hacking para el año 2024, donde se valide la remediación de las vulnerabilidades reportadas y se identifique nuevas vulnerabilidades.
- 
- Darle la importancia necesaria 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.
- 
- Adjunto al presente informe se encuentra la matriz de vulnerabilidades, la cual compone todas las estadísticas actualmente presentadas.

## 10. Gestión de la continuidad de Negocio

a. La OTI fue designada como la encargada de establecer el PLAN DE CONTINUIDAD DE NEGOCIO (BCP), 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. En Caso de que efectivamente se ratifique a la OTI, se debe establecer el ROL de líder de Continuidad, quien es el encargado de establecer los lineamientos para las diferentes áreas incluyendo el PRD que está en liderazgo del Oficial de seguridad de la información.

c. La Agencia Nacional de Minería estableció un proyecto de hiperconvergencia como resultado del anterior análisis PRD para las plataformas críticas ANNA Minería, SGD, Control a la Producción, WEBSAFI y RUCOM. Los nodos establecidos en esta infraestructura de TI permitirán tener un plan de recuperación de desastres tecnológico para estas plataformas críticas. Priorizando estas plataformas establecidas en el Analisis de impacto BIA.

d. Para los sistemas de información o plataforma tecnológica que no quedarán soportados por estos nodos de hiperconvergencia que están en el noveno piso de la sede principal de la Agencia Nacional de Minería, se debería establecer un plan de recuperación de desastres tecnológico con la plataforma cesante del proyecto de hiperconvergencia.

e. Otro factor crítico que se evidencia en la Agencia Nacional de Minería, son las carpetas compartidas de los procesos y grupos, sin embargo, la migración que se establece actualmente cargados en SharePoint. Como mecanismo se habilitó el DLP de esta plataforma para mantener histórico de datos. No obstante, es importante aclarar que Estos repositorios actualmente no poseen plan de contingencia.

f. Es importante que, como parte del proceso de mejora continua en la Agencia Nacional de Minería, realice por lo menos una vez al año auditorías internas. Así mismo, entregar informes al Comité de Gestión y Desempeño de la Gestión del Plan de Continuidad de Negocio, del estado de la implementación de las estrategias, del nivel de sensibilización de la ANM, el grado de capacitación del personal y los resultados de las pruebas para que se puedan tomar acciones preventivas y correctivas que mejoren la respuesta de resiliencia frente a un incidente y la operación en un ambiente alterno.

g. La Alta Dirección de la Agencia Nacional de Minería, debe contemplar por lo menos una vez al año la revisión de los lineamientos y parámetros consignados en el presente manual, el estado de las acciones de las revisiones anteriores, cambios que puedan afectar el PCN, acciones correctivas y los resultados de la auditoría.

h. Además de realizar la actualización documental, la capacitación de los integrantes del BCP, se debe colocar en un repositorio público los contactos de los integrantes y un breve instructivo de su rol dentro del proceso, esto con el ánimo de facilitar las labores

i. Es necesario actualizar el PRD y a su vez establecer un plan de trabajo con el equipo de la OTI para su implementación y pruebas en el periodo 2024.

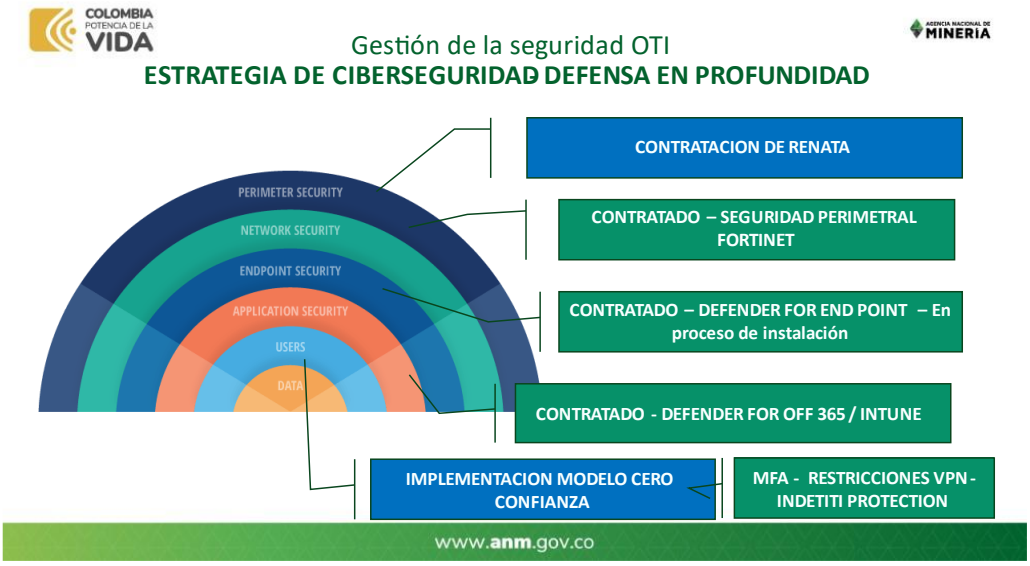
## 11. Actividades específicas para el año 2024

- Formalización de procedimiento para la gestión de usuarios en aplicaciones

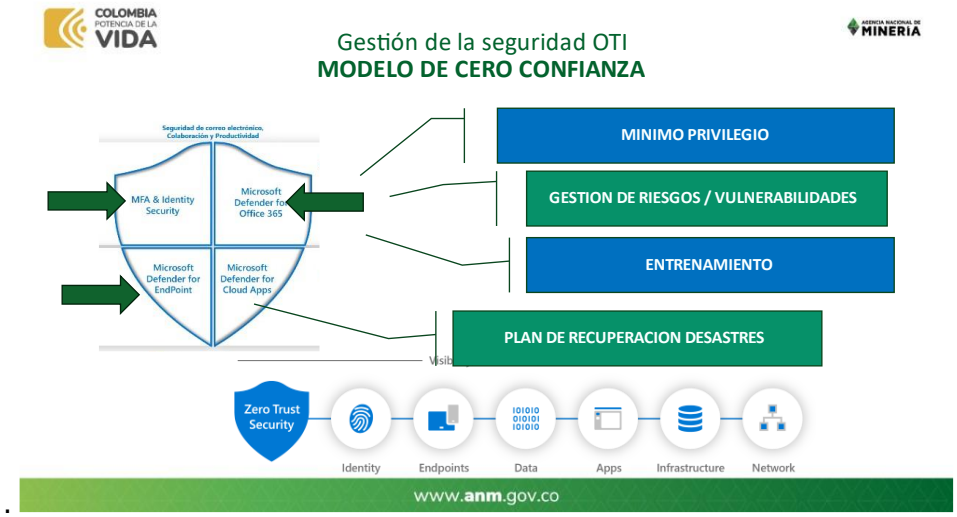
- Se debe reforzar los controles de auditoría para que terceros también tengan programas de protección de end point profesional para el acceso a las redes de la entidad.
- Se deben reforzar las políticas de red apuntando a la microsegmentación de las redes virtuales VLAN.

- Se debe implementar 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 con el proveedor RENATA.




- Se debe establecer las acciones que aporten la estrategia de confianza cero (Zero Trust) en las diferentes etapas




- 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

| Versión | Fecha del cambio | Descripción de la modificación |
|---|---|---|
| 1 | 12 de enero de 2020 | Creación. |