Plan de Seguridad y Privacidad de la Información

Versión 1: enero 2021

Contenido

1. INTRODUCCIÓN 2
2. OBJETIVO 2
2.1. Objetivos Específicos 2
3. ALCANCE 3
4. DEFINICIONES 3
5. JUSTIFICACIÓN 4
6. ANTECEDENTES 8
6.1. Marco de Gestión de la Seguridad de la Información y Ciberseguridad 9
6.2. Política de Seguridad de Información 9
6.3. Gestión de Inventario de Activos de Información 12
6.4. Gestión de Riesgos de Seguridad 13
6.5. Plan de Capacitación y Concienciación 16
6.6. Gestión de Incidentes de Seguridad de la Información 17
6.7. Programa de Gestión de la Documentación del SGSI y Ciberseguridad 19
6.8. Gestión de Vulnerabilidades Técnicas 22
6.9. Continuidad de Negocio 23
7. Medición del Modelo de Seguridad y Privacidad de la Información 27
8. Cronograma de Actividades 27
9. Conclusiones 29
Anexo 1 Control de Cambios 30

1. INTRODUCCIÓN

El Plan de Seguridad Digital y Privacidad de la Información, establece un análisis de brecha con el fin de determinar el nivel de madurez del Sistema de Gestión de Seguridad de la Información norma NTC ISO/IEC 27001:2013 y las acciones a implementar para reducir dichas brechas.

Se toma como base la documentación desarrollada por la Oficina de Tecnología e Información que se tiene actualmente, el conocimiento de las personas frente al Sistema de Gestión de Seguridad de la Información y un análisis de todos los dominios de la norma NTC ISO/IEC 27001:2013 establecidos en la Declaración de Aplicabilidad para su implementación como parte de los controles para mitigar el riesgo de exposición de la información a las amenazas cibernéticas.

Es así como, el Plan de Seguridad y Privacidad de la Información y Ciberseguridad de la Agencia Nacional de Minería, está alineado al cumplimiento de la normativa de Gobierno Digital y Seguridad Digital, y se enfoca en acciones para la protección de los activos críticos de información, contrarrestando las amenazas y riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

2. OBJETIVO

Identificar e implementar acciones orientadas a fortalecer el aseguramiento de los activos de información, que soportan la operación en la Agencia Nacional de Minería (ANM), y que mediante el fortalecimiento de los servicios de TI, se preserve la confidencialidad, integridad y disponibilidad de la información de la Entidad.

2.1. Objetivos Específicos

1. Fortalecer el aseguramiento de los activos de información, suministrada o relacionada con los titulares mineros, mediante las exigencias que se imparten a través del Modelo de Seguridad y Privacidad de la Información y, en el marco legal de la Ley 1581 de 2012.

2. Fomentar en los procesos de la Entidad, la gestión de la seguridad de la información, su uso y apropiación para la mejora continua preservando la seguridad en la información.

3. Ejecutar actividades a través del Sistema de Gestión de Seguridad y Privacidad de la Información y, establecer así, un modelo de madurez aplicable y repetible frente a las acciones con la seguridad de la información.
4. Socializar las políticas, los lineamientos en los procedimientos, las buenas prácticas y recomendaciones que permitan establecer una cultura para la gestión del Sistema de Seguridad de la Información.

3. ALCANCE

La Agencia Nacional de Minería, genera, obtiene, almacena, intercambia, divulga y actualiza información clasificada, reservada y pública, relacionada con los titulares mineros, sus funcionarios, contratistas y/o terceros contratados por proveedores.

Esta información se considera un activo de valor para la Entidad, registrando esta información en un contexto histórico y de privacidad, frente a las partes interesadas; Como:

- Titulares de Derechos Mineros
- Entidades Nacionales
- Entidades Territoriales
- Sociedad y Comunidad Internacional
- Cliente Interno

4. DEFINICIONES

Activo de Información: Cualquier elemento que soporta uno o más procesos del negocio, con información definible e identificable, almacenada en cualquier medio y que tiene valor para la ANM, por lo tanto, debe protegerse.

Amenaza: Circunstancia potencial, evento o persona que puede manifestarse en un lugar y momento específico de forma voluntaria o involuntaria y que tiene el potencial de causar daño a un sistema de información de la Entidad.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo para poder estimar o determinar su nivel. Este análisis provee las bases para la evaluación del riesgo y las decisiones requeridas para implementar su tratamiento.

Ciberespacio: Entorno donde las entidades que están conectadas a la red informática mundial de internet, interactúan.

Confidencialidad: Característica de los activos de información que determina que éstos sólo sean revelados a individuos, procesos, áreas o entidades autorizadas.

Control de Seguridad: Procedimiento, práctica o actividad estructurada, definida para mantener los riesgos de seguridad y privacidad de la información, por debajo de los niveles aceptables.

Disponibilidad: Característica de los activos de información que determina que éstos accesibles y utilizables, cuándo y cómo se requieran, para solicitud de una persona o ente autorizado.

Integridad: Característica de los activos de información que determina que éstos se salvaguarden con exactitud y en completo estado.

Norma NTC-ISO/IEC 27001:2013: Es la versión del año 2013 de la norma ISO 27001 que "proporciona los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información".

Norma NTC-ISO/IEC 27002:2013: Es la versión del año 2013 de la norma ISO 27002 que "está diseñada para que las organizaciones la usen como un marco de referencia para seleccionar controles dentro del proceso de implementación de un sistema de gestión de la seguridad de la información".

Riesgo: Probabilidad existente que una amenaza pueda explotar una vulnerabilidad y causar un daño a los servicios informáticos de una organización, incluyendo la información existente en estos servicios.

Seguridad de la Información: Gestión de las medidas y controles diseñados para el tratamiento de los riesgos generados por la afectación de la confidencialidad, integridad y/o disponibilidad de los activos de información de una organización de acuerdo con la política de gestión de riesgos aprobada por la Dirección General. Estas medidas y controles incluyen: políticas, procedimientos, guías de implementación, estándares, soluciones de software y hardware, controles electrónicos, capacitación y concienciación.

5. JUSTIFICACIÓN

El Estado Colombiano, cuenta con normativa vigente que obliga el adecuado tratamiento de la información (creada, almacenada y transportada) por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras que se citan a continuación:

a. **Ley 1437 de 2011, Capítulo IV,** *"utilización de medios electrónicos en el procedimiento administrativo".*
"Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."

b. **Ley 1581 de 2012**, *Principio de seguridad:*
"La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente Ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."

c. **Ley 1581 de 2012, Artículo 17, ítem d**: "*Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*"

d. **Ley 1712 de 2014**, "*principio de transparencia*":
"*Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta Ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la Ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta Ley.*"

e. **Ley 1712 de 2014, artículo 7**: "*Disponibilidad de la información*"
"*En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente Ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones.*

Así mismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

f. **Ley 1712 de 2014** -Título III "*Excepciones acceso a la información*"
"*Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito.*"

g. **Decreto 2573 de 2014:** *"Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea…" donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.*

h. **Decreto 1413 de 2017**, artículo 2.2.17.6.6, "*Seguridad de la información.*"
"*Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.*"

i. **Decreto 1413 de 2007**, artículo 2.2.17.6.1, "*responsable y encargado del tratamiento"*:
"Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen."

j. **Artículo 2.2.17.6.3**, "*Responsabilidad demostrada*".
"*Los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.*"

k. **Decreto 1413 de 2007**, artículo 2.2.17.6.5, "*Privacidad por diseño y por defecto*":
"Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy lmpact Assessment (PIA), cuyo objetivo se dirige a que la protección

de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador".

l. **Decreto 1413 de 2017, artículo 2.2.17.5.10**, *"Derechos de los usuarios de los servicios ciudadanos digitales":*
"Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador.

a. Aceptar, actualizar y revocarlas autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales.

b. Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre.

c. Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación a los servicios ciudadanos digitales.

d. Elegir y cambiar libremente el operador de servicios ciudadanos digitales.

e. Solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su retiro de la plataforma de servicios en· cuyo caso podrá descargar su información a un medio de almacenamiento propio.

m. **Decreto 1413 de 2017, artículo 2.2.17.2.1.1** *"Descripción de los servicios ciudadanos digitales, 1.5 servicio de interoperabilidad:*
Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicos cuando lo requieran."

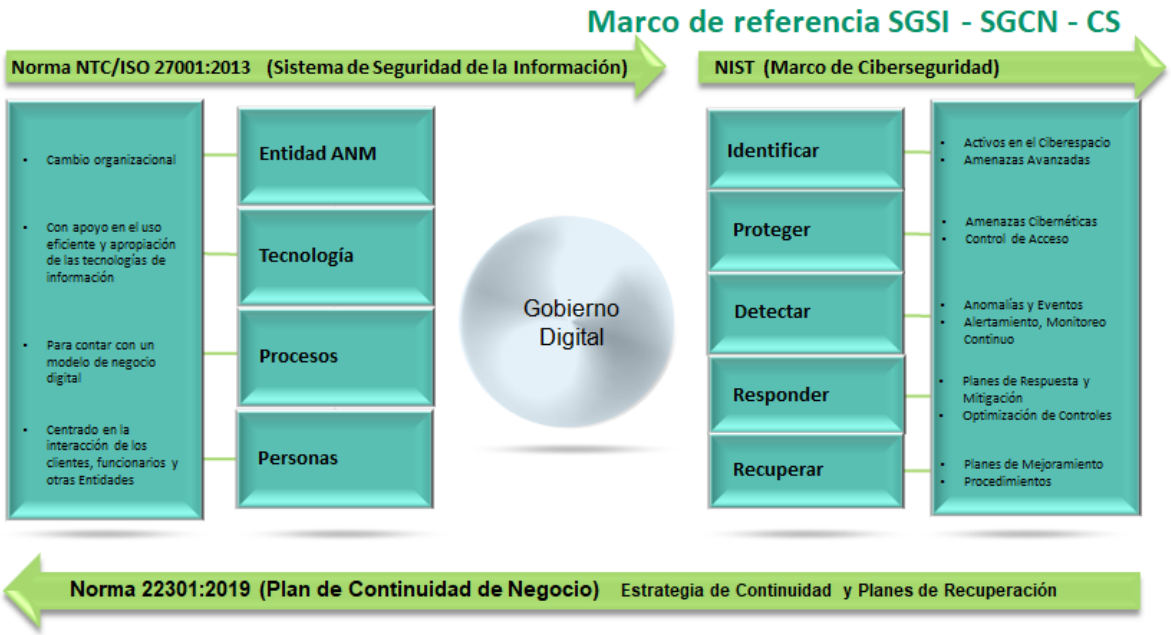
n. **Decreto 612 de 2018, artículo 1.** *"Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web."*

o. **CONPES 3854 de 2016, objetivo general** *"Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país".*

Por lo anterior, la Agencia Nacional de Minería, debe emprender acciones orientadas a la protección de la información (creada, almacenada y transportada), realizando la identificación, valoración y tratamiento de riesgos de la información y ciberseguridad de los activos críticos que la soportan, de manera que se establezca el seguimiento a dichas acciones en un marco del plan de acción de cumplimiento a los lineamientos del Sistema Integrado de Gestión.

6. ANTECEDENTES

6.1. Marco de Gestión de la Seguridad de la Información y Ciberseguridad



Fuente: Imagen original de la ANM

6.2. Política de Seguridad de Información

Por medio de la Resolución 534 del 25 de noviembre de 2020, firmada por la Presidencia de la ANM, se adoptan las políticas del Sistema Integrado de Gestión donde se establece el subproceso de Seguridad de la Información y Ciberseguridad, siendo ésta de cumplimiento por parte de directivos, funcionarios, contratistas y terceros que accedan, almacenen o transporten la información de la ANM.

La Agencia Nacional de Minería, Entidad aliada al desarrollo sostenible del país a través de la generación de valor, con una gestión moderna, transparente y eficiente de los recursos minerales de los colombianos, está comprometida con el cuidado y gestión adecuada de la información propia de los titulares mineros y ciudadanos mediante la implementación, operación y mejora continua de un sistema de gestión de seguridad de la información (SGSI), orientado a mantener y preservar los principios fundamentales de Confidencialidad, Integridad y Disponibilidad de la información.

Esta política puede ser consultada a través del siguiente link:

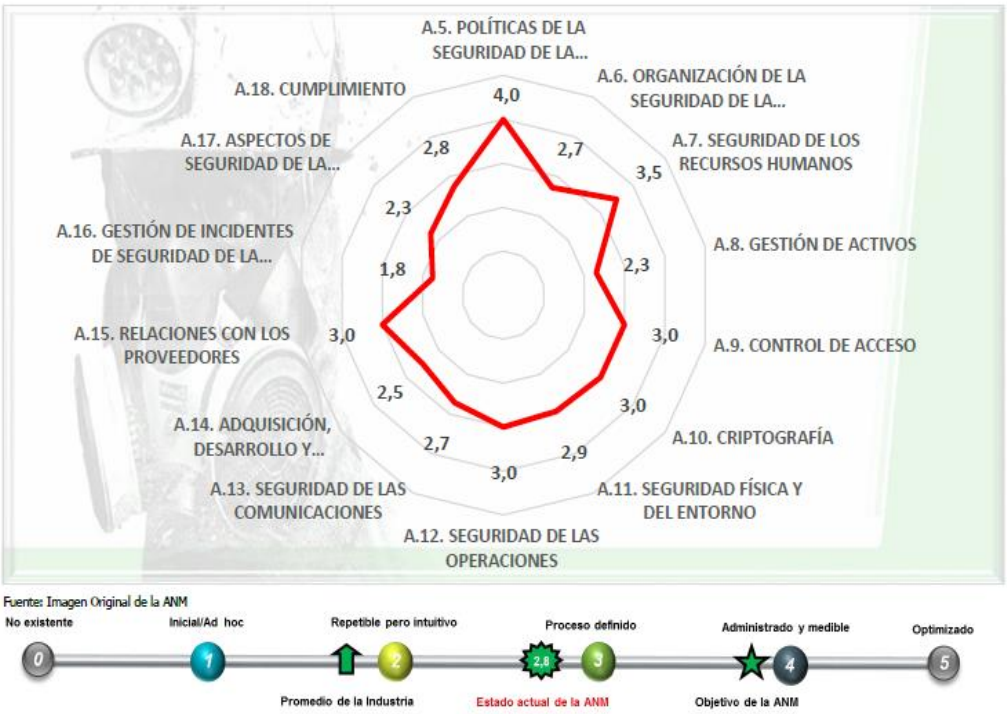
https://www.anm.gov.co/sites/default/files/resolucion_534_de_25_noviembre_2020.pdf

Adicionalmente, para conocer más acerca de esta política y su aceptación como colaborador y proveedor de la ANM ingresa al siguiente link.

https://survey123.arcgis.com/share/76f895e64ff74aa4bc6a732240cc157e

Dentro del marco del Modelo de la Seguridad y Privacidad de la Información que se evaluó entre el diciembre de 2019 a Enero 2020, se desarrollaron diferentes iniciativas que han permitido evidenciar el nivel de madurez del Sistema de Gestión de Seguridad de la Información con lo que se venía trabajando en el SGSI en los años anteriores por citar (año 2019), un aspecto importante en todo su ámbito y en pro de la mejora continua del sistema de seguridad de la información, dando como resultado el siguiente nivel de madurez 45.5%.

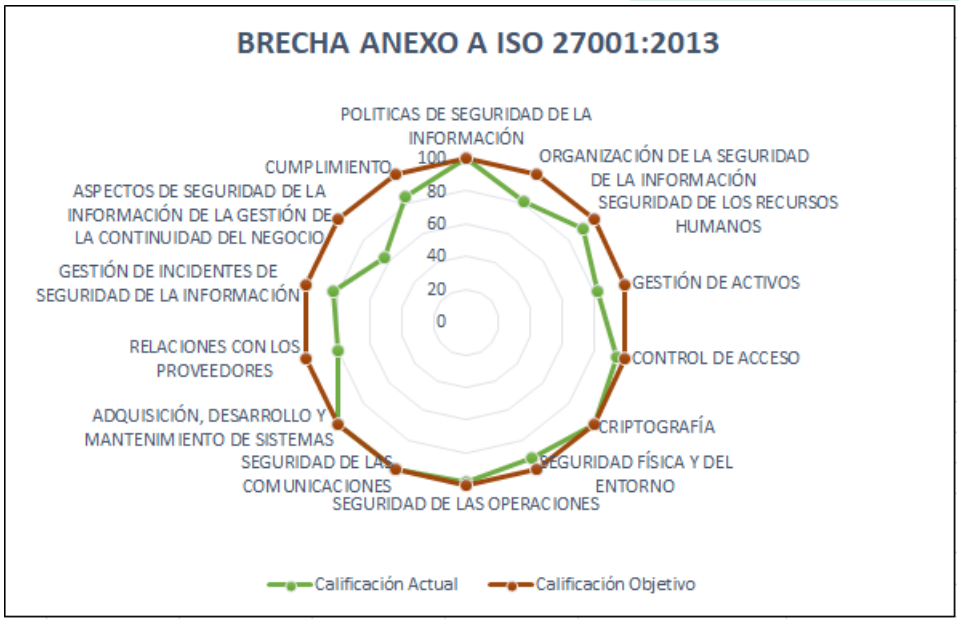
0- No se aplican procesos administrativos en lo absoluto
1- Los procesos son ad-hoc y desorganizados
2- Los procesos siguen un patrón regular
3- Los procesos se documentan y se comunican
4- Los procesos se monitorean y se miden
5- Las buenas prácticas se siguen y se automatizan



Es así que implementar el SGSI en la Agencia Nacional de Minería durante el año 2020, permitió concretar cada uno de los objetivos trazados en el Plan de Seguridad y Privacidad de la Información ejecutado en el año 2020, logrando así contar con un nivel de madurez mucho más eficiente y medible que permite evidenciar dicha gestión a través de la implementación del Sistema de Gestión de Riesgo y Cumplimiento GRC, que se implementó desde el Ministerio de Minas y Energía.

Medición que permite evidenciar una vez más la gestión realizada por la Oficina de Tecnología e Información dentro del marco del PETIC y el PESI que se estructuró para el año 2020 arrojando un índice favorable en la medición de la evaluación de la implementación del Modelo de Seguridad y Privacidad de la Información del MinTIC - MSPI, como se aprecia a continuación:

BRECHA ANEXO A ISO 27001:2013

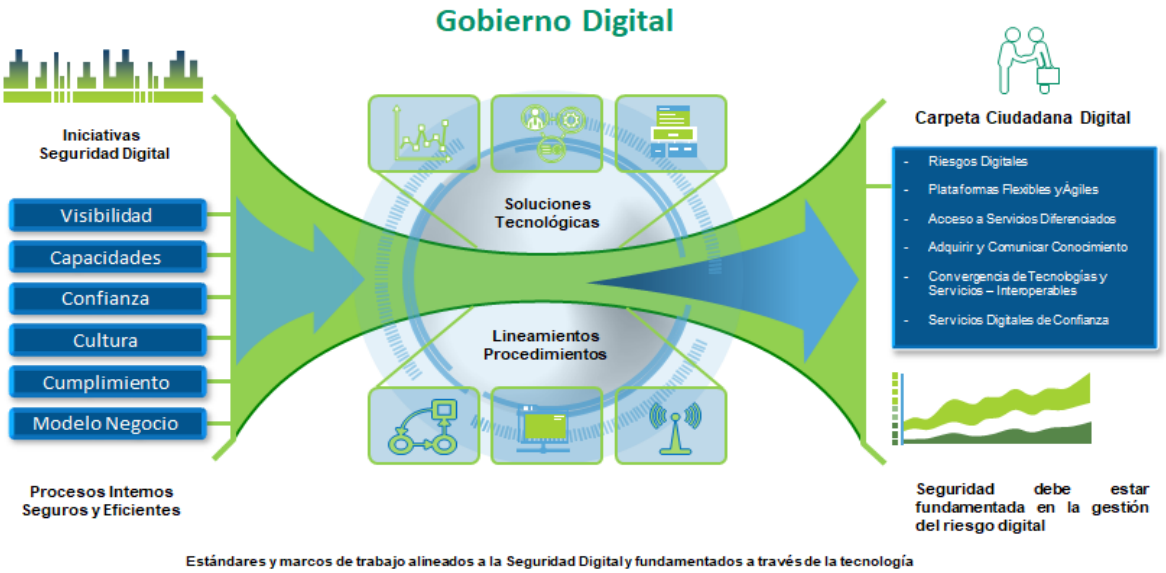


Fuente: Imagen original de la ANM

Se evidencia un promedio total de 89% en la evaluación de los controles de la Norma NTC/ISO27001:2013 con respecto al 45.5% del año 2019.

El dominio que presenta menor nivel de avance, es el de aspectos de seguridad de la información en la gestión de la continuidad de negocio. Frente a este dominio se esperan importantes avances para el año 2021, a través de la nueva infraestructura que adquirió la Entidad, desde la Oficina de Tecnología e Información llamada Hiperconvergencia.

Es así que a continuación se citan grandes iniciativas que deben continuar su gestión para el año 2021 como mejora continua del SGSI y como parte de la implementación del Plan de Seguridad y Privacidad de la Información para la mitigación del Riesgo de Seguridad encaminadas en una postura que responden a los lineamientos que se establecen igualmente desde el marco de Gobierno Digital.



Fuente: Imagen original de la ANM

Entre éstas están:

6.3. Gestión de Inventario de Activos de Información

En el año 2020, en el marco del Sistema Integrado de Gestión y el Subsistema de Gestión de Seguridad de la Información, los procesos de la Entidad realizaron el levantamiento de los activos de información con base en la matriz de registro de activos de información.

Este insumo permitió dar cumplimiento a lo establecido en la Ley 1712 de 2014, respecto a la generación y publicación de los siguientes instrumentos:

- Registro de activos de información
  https://www.anm.gov.co/?q=registro-de-activos-de-informacion

- Registro del Índice de información clasificada y reservada
  https://www.anm.gov.co/?q=indice-de-informacion-clasificada-y-reservada

Esta actividad permitió la identificación, clasificación y valoración de criticidad de activos tipo información, software y hardware en los procesos, bajo una metodología documentada y aprobada por la Entidad, desarrollada desde el equipo de seguridad de la información para su aprobación por parte del proceso de gestión documental.

Esta matriz puede ser consultada a través del siguiente link, dando así cumplimiento a la Ley 1712 de 2014 Ley de Transparencia:

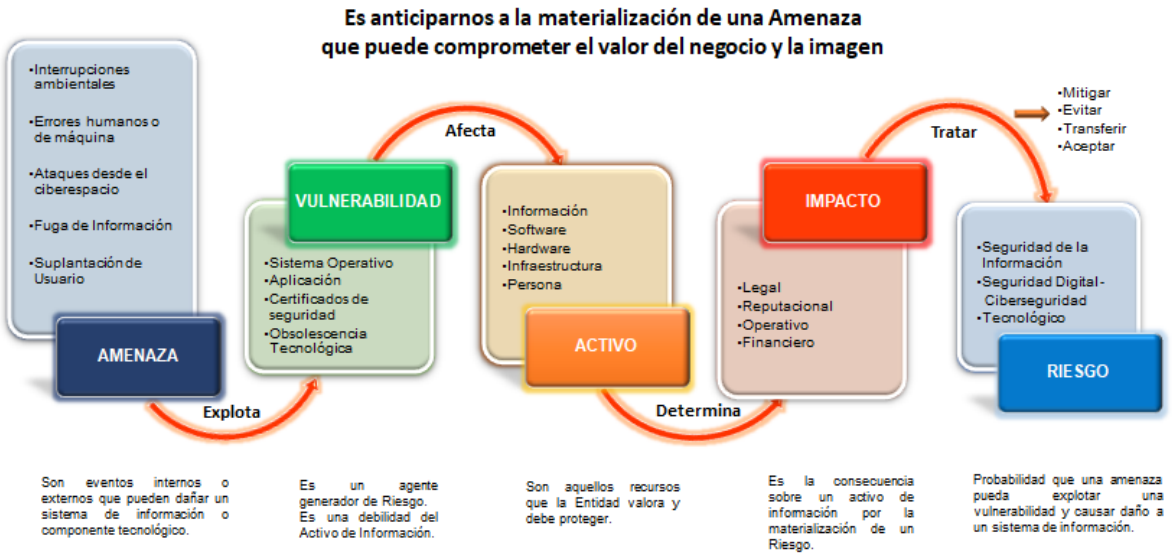
https://www.anm.gov.co/sites/default/files/DocumentosAnm/registro_activos_informacion_2020v2.xlsx

Conforme a lo anterior es importante dar continuidad a esta gestión de identificación y valoración de activos de información en cada uno de los procesos que ya cuentan con esta matriz de inventario de activos de información, como tal, es conveniente su actualización durante este año 2021 conforme lo establece el procedimiento de Gestión de Activos de Información de la ANM.

6.4. Gestión de Riesgos de Seguridad

En el año 2020, teniendo en cuenta las actividades ejecutadas en periodos anteriores, la Oficina de Tecnologías e Información generó la matriz de riesgos de seguridad de la información, alineada a la Metodología de Administración Gestión de Riesgos de la Entidad.

MARCO DE GESTIÓN Y DIRECCIÓN DEL RIESGO DE SEGURIDAD DIGITAL



Fuente: Imagen original de la ANM

Conforme a lo anterior, crear un perfil actual (as is) es parte fundamental, porque nos ayuda a cambiar la forma de direccionar la Entidad en el cumplimiento de los objetivos estratégicos y llegar así a establecer un perfil deseado (to be), con el

propósito de anticiparnos a la materialización de una amenaza que pueda comprometer el valor de la Entidad y la Imagen.

Algunos beneficios que se dan a conocer basados en esta identificación y evaluación del Riesgo de Seguridad se describen a continuación:

a. Cumplimiento Normativo
b. Transformación Digital
c. Cultura en la gestión del riesgo digital
d. Monitoreo continuo
e. Estrategia para la toma de decisiones

Todos los procesos de la Entidad, están expuestos al riesgo de seguridad en la información y Ciberseguridad. De ahí la importancia de conocer estos riesgos y la implementación debida y eficiente de los controles para minimizar su impacto.

Fuente: Imagen original de la ANM

La agestión del riesgo es una actividad holística que está totalmente integrada en todos los aspectos y procesos en las operaciones de la Entidad. Es así que, La Agencia Nacional de Minería, es consciente de la importancia de llevar una gestión de riesgos desde cada uno de sus procesos de negocio, por tanto, esta iniciativa tiene en consideración, aquellos requisitos de negocio y que están relacionados con la seguridad de la información y tienen como finalidad la reducción de los mismos a través de los planes de tratamiento dispuestos a poner en ejecución e implementación en el año 2021 definiendo las acciones a contemplar en la documento **Plan de Tratamiento de Riesgos 2021 ANM**.

No obstante, para el año 2021 se debe priorizar una cultura en la gestión del riesgo de seguridad de la información y ciberseguridad, contando con un gestor en cada uno de los procesos, para la debida gestión en la aplicación de los planes de tratamiento del riesgo digital, y que se han definido en la Matriz del Riesgo de Seguridad Digital, aprobada por el Comité de Gestión y Desempeño de la Entidad.

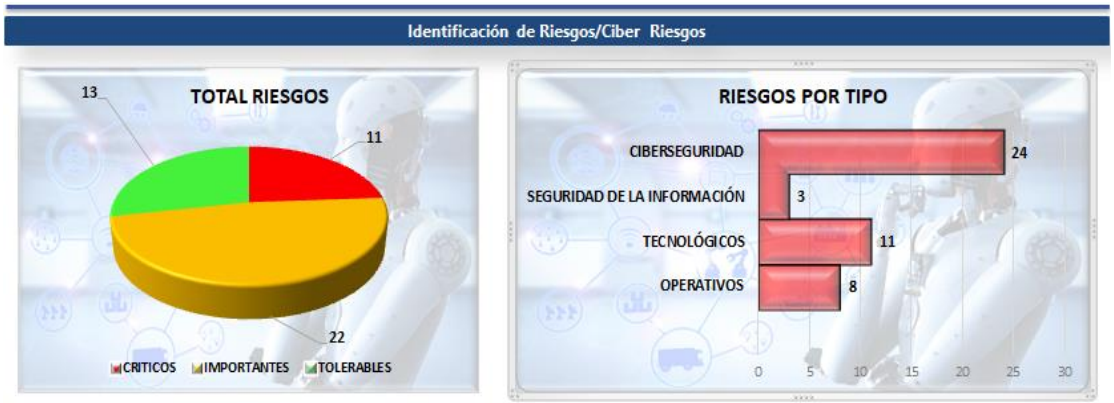
Se determinan qué factores pueden suceder en el entorno del ciberespacio como posibles amenazas internas o externas y, que pueden ser causa de pérdidas potenciales a nivel **financiero, legal y reputacional**.

Se determina qué controles de seguridad son fundamentales, ya que sin éstos, los riesgos que están por encima del **Nivel de Riesgo Aceptable** (NRA) conllevarán en pérdidas a los procesos de la Entidad.

Adopta nuevos procedimientos que establecen un nivel adecuado y requerido para las **oportunidades de mejora,** preservando la confidencialidad, integridad y disponibilidad de los activos de información.

En la gestión del Riesgo de Seguridad de la Información, el activo a proteger es la información. Es decir que la gestión y aplicación de los planes de tratamiento del riesgo se deben ocupar de todo el ciclo de vida de la información, considerando aspectos como la creación, almacenamiento y el transporte de ésta y, así como, la destrucción de la misma.

En el marco de la metodología de riesgos establecida por el Grupo de Planeación de la Agencia Nacional de Minería, en el año 2020, se identificaron planes de tratamiento para mitigar el riesgo digital dentro de este marco. Sin embargo, siendo ésta una actividad compleja e integral, que requiere la participación de todos los funcionarios de la Entidad, es necesario contar con la documentación específica que requiere cada una de las etapas para el tratamiento de los riesgos, en este caso se tomará la metodología usada actualmente para llevar a cabo su implementación con el apoyo de los gestores del riesgo definidos en cada uno de los procesos.



Fuente: Imagen original de la ANM

Llevar a cabo este análisis de riesgos ha permitido identificar las medidas de seguridad importantes para cada uno de los procesos y operación de la Entidad, dado que la materialización en el tiempo de alguno de estos riesgos, implica un problema por:

a. Multas por incumplimiento al no contar con disponibilidad de la información
b. Incremento en los deducibles de los seguros por la reclamación
c. Incremento en costos para:
   - ✓ Contener,
   - ✓ Reparar,
   - ✓ Recuperar las operaciones de negocio.

Dichos controles definidos en cada uno de los riesgos, son relevantes para la mitigación de éstos riesgos de seguridad que posteriormente se puedan llevar a un plan de monitoreo, para medir su eficiencia y eficacia.

6.5. Plan de Capacitación y Concienciación

Es de resaltar que uno de los aspectos más importantes en la gestión del año 2020, evidenciado desde la gestión del Sistema de Seguridad de la Información, fue haber logrado una sinergia que se traduce en acciones colaborativas desde todos los funcionarios y contratistas de la Entidad, permitiendo que esta gestión sea íntegra desde todos sus procesos y, eficiente para el fortalecimiento de la Seguridad Digital y Ciberseguridad. Acciones fundamentadas en preservar la Confidencialidad, Integridad y Disponibilidad de la información en la Agencia Nacional de Minería, permitiéndole ser una Entidad más Resiliente.

Sin embargo, el plan de capacitación y concienciación con respecto a la Seguridad y Privacidad de la Información y Ciberseguridad debe ser una iniciativa constante, que busque disminuir la brecha actual en los funcionarios de la Agencia Nacional de Minería, frente a las responsabilidades con la Seguridad de la Información tanto digital como física, en donde la OTI planteará temas diferentes con propuestas en:

- ✓ Charlas fundamentales en Seguridad y Privacidad de la Información y Ciberseguridad
- ✓ Capacitaciones a los funcionarios y contratistas en los temas relacionados con el sistema de gestión de la seguridad de la información.
- ✓ Socializar las Políticas del Manual de Seguridad de la Información.
- ✓ Conceptos de Gobierno de Protección de Datos Personales.

- ✓ Amenazas Cibernéticas (Phishing, Malware, Ramsonware, etc.)
- ✓ Ingeniería Social.
- ✓ Tips de Seguridad con la Información.

A continuación puede usted visualizar algunos de los aspectos que se han contemplado como Tips de seguridad en la Agencia Nacional de Minería a través de la Intranet desde el siguiente link:

https://anmgovco.sharepoint.com/sites/Intranet/oti/Paginas/tips_sg.aspx

6.6. Gestión de Incidentes de Seguridad de la Información

En la Agencia Nacional de Minería, se encuentra afianzado el manejo de la gestión de incidentes tecnológicos desde la Oficina de Tecnología e Información.

Es así que, se fortalecerá el procedimiento de gestión de incidentes para que se incluya la gestión de incidentes de seguridad de la Información, con el fin de ser más predictivos frente a las amenazas del ciberespacio que bien se pueden traducir en:

Ataques desde el ciberespacio:

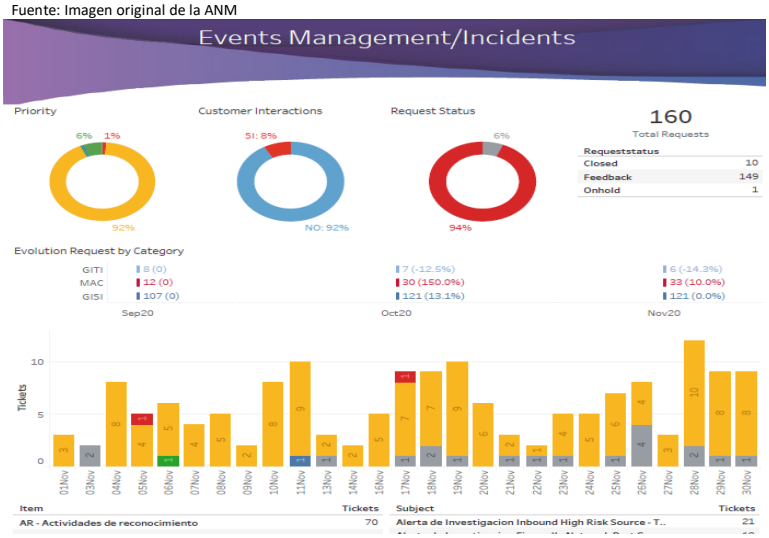
Se debe evaluar la combinación de amenazas, vulnerabilidades e impacto a fin de identificar tendencias importantes para aplicar un esfuerzo en eliminar o reducir las capacidades de estas amenazas sofisticadas que cada día surgen en el ciberespacio, entre éstas se encuentran:

- ✓ Interceptación de canales de comunicaciones (Espionaje remoto o escucha).
- ✓ Hurto o fuga de archivos o información.
- ✓ Divulgación no autorizada de información.
- ✓ Datos provenientes de fuentes no confiables (Phishing, Malware, Ransomware, etc.).
- ✓ Acceso no autorizado a la información.
- ✓ Modificación no autorizada de la información.
- ✓ Copia fraudulenta del Software.
- ✓ Corrupción de datos.
- ✓ Abuso o falsificación de derechos de autor.

Adicionalmente, para el año 2021 entrará en operación el módulo de gestión de incidentes que se desarrolló en el año 2020 desde la plataforma de gestión de Mesa de Ayuda de la Entidad.

Desde el SOC que la Agencia Nacional de Minería tiene como servicio, se permite conocer en todo momento la disponibilidad y el rendimiento de toda la infraestructura tecnológica a través de las plataformas de seguridad, de redes y comunicaciones, siendo proactivos identificando acciones o patrones de comportamiento fuera de lo habitual que se traducen en eventos de seguridad.

Fuente: Imagen original de la ANM



Dentro de sus beneficios más importantes en esta gestión se pueden resaltar los siguientes:

A. Detectar y corregir comportamientos anómalos

A través de las plataformas de seguridad que provee el SOC como servicio para la Agencia Nacional de Minería.

B. Gestionar la calidad del servicio con eficiencia y exactitud

A través de indicadores de gestión de eventos de seguridad, que permiten visualizar el estado del servicio que presta la infraestructura tecnológica de la Agencia Nacional de Minería.

C. Visualización óptima y asertiva

Representada en gráficas, lo que permite hacer un análisis de correlación comprobando las capacidades de seguridad a través de logs.

Contar con estas plataformas de seguridad, permiten diferenciar un enfoque de estado conocido de un estado en busca de desviaciones que realizan una acción como respuesta a una determinada condición, como lo han sido tradicionalmente

los sistemas IDS/IPS, capacidades que se traducen en crear reglas óptimas y asertivas que ayuden en la entrega de información oportuna y eficiente.

Conforme a lo anterior, en el año 2020, los colaboradores de la Agencia Nacional de Minería, dieron a conocer sus inquietudes frente a situaciones anormales que se presentaron con la información especialmente en temas de confidencialidad e integridad, lo que permite ver un alto compromiso y apoyo con la Gestión del Sistema de Seguridad de la Información, tales como:

a. ASPANM (Tema de Confidencialidad e Integridad)
b. PAR Bogotá (Tema de Disponibilidad)
c. PAR NOBSA (Tema de Confidencialidad)
d. Control Disciplinario (temas de Acceso no Autorizado)

Todas estas acciones se establecen como eventos materializados que se traducen en la debida Gestión de Incidentes de Seguridad de la Información. Lo que indica que las capacitaciones y planes de concienciación que se ejecutaron en el 2020 desde la Oficina de Tecnología e Información, respondieron con un alto nivel de participación y de acciones colaborativas por parte de los usuarios.

Dentro de este Plan de Seguridad y Privacidad de la Información es importante resaltar que para el año 2021 es necesario formar un equipo de trabajo en la respuesta de incidentes de seguridad y gestión de crisis, con el propósito de dar respuesta oportuna a los incidentes que se materialicen y que puedan poner en riesgo la información propiedad de la Agencia Nacional de Minería.

La importancia de contar con este equipo CSIRT, que permita gestionar de manera eficiente la administración de los procesos de TI y, de cumplimiento regulatorio para el SGSI para anticiparnos a las amenazas del ciberespacio.

6.7. Programa de Gestión de la Documentación del SGSI y Ciberseguridad

Es de resaltar que uno de los aspectos importantes en todo el Sistema de Gestión de Seguridad de la Información y Ciberseguridad, es la documentación que se desarrolla y que es requisito para contemplar lineamientos y aspectos de seguridad para su aplicación desde la operación de la Entidad.

Es así que, en el año 2020, se llevó una gestión en el desarrollo y actualización de la documentación del SGSI y procedimientos para la operación de los procesos de TI.

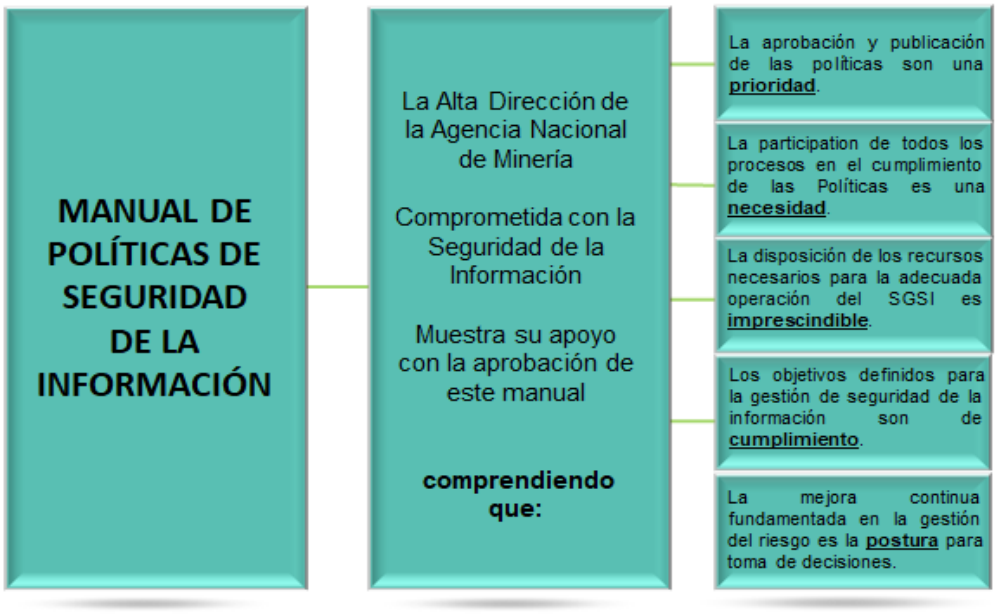
No.	Documentos SGSI
1	Procedimiento de Intercambio Seguro de Información
2	Procedimiento de Borrado Seguro
3	Instructivo de Seguridad Cifrado
4	Manual Adquisición, Desarrollo y Mantenimiento de Sistemas
5	Procedimiento Respuesta a Incidentes y Crisis
6	Procedimiento Gestion de Activos
8	Procedimiento Gestion de Vulnerabilidades
10	Procedimiento Evidencia Digital
11	Procedimiento Gestion de Proveedores
12	Metodologia Declaracion de Aplicabilidad - SOA
15	Manual Organización de Seguridad de la Informacion
16	Procedimiento Derechos de Propiedad Intelectual
17	Procedimiento dar de baja un Software
19	Procedimiento Gestion de la Configuración
20	Procedimiento de Gestión de la Capacidad
21	Procedimiento de Backups
	Documentos Continuidad de Negocio
1	Analisis de Impacto al Negocio_BIA_ANM_Dic22
2	Manual Gestion Continuidad del Negocio_PCN_ ANM_Dic22
3	Politica Continuidad de Negocio_Dic22
4	Plan de Recuperacion de Desastres_DRP_Control a la producción_Dic22
5	Plan de Comunicacion de Crisis_Dic22
6	Plan de Pruebas_Control a la Produccion_Dic22
7	Informe_resultado_pruebas_Control a la Produccion_Dic22

Sin embargo, algunos de estos documentos, continúan con ajustes que, para el 2021 deben quedar aprobados por la Oficina de Planeación y publicados desde el Sistema de Gestión de Calidad.

Adicionalmente, la Oficina de Tecnología e Información, permitió llevar acabo la reunión con todos los directivos del Comité de Gestión y Desempeño, dando a conocer a esta directiva, la importancia de cada una de las políticas que se establecieron desde el Manual de Seguridad de la Información y, el liderazgo y compromiso que la Agencia Nacional de Minería tiene bajo su responsabilidad de mantener y velar por el buen uso y apropiación de la estas políticas.

A continuación se dan a conocer los aspectos generales de cada una de las políticas del Manual de Seguridad de la Información a través del siguiente link:

https://anmgovco.sharepoint.com/sites/Intranet/oti/Documents/ManualPoliticas2.pdf



La información para la Entidad es un diamante a proteger

Para consultar el Manual de Políticas de Seguridad de la Información ingresa a través del siguiente link:

https://isolucion.anm.gov.co/IsolucionANM/BancoConocimientoANM/c/cfb8704491894fe1be592ad9f1d8d87d/ANEXO7.MANUALPOLITICASDESEGURIDADDELAINFORMACION.pdf

Fuente: Imagen original de la ANM

6.8. Gestión de Vulnerabilidades Técnicas

Las pruebas de Ethical Hacking y el análisis de vulnerabilidades son medios útiles para determinar el nivel de exposición que poseen la infraestructura tecnológica y de las aplicaciones evaluadas, una evaluación periódica permite obtener resultados positivos que contribuyen a acreditar el nivel de seguridad de la arquitectura tecnológica.

El análisis de vulnerabilidades, permite además, establecer una línea base para el mejoramiento continuo de los objetivos de la seguridad de la información y ciberseguridad, orientado a esfuerzos de mejora continua.

La metodología utilizada por el proveedor DIGIWARE, se basa en un enfoque de trabajo que va de lo general a lo particular y está soportada con bases de conocimiento y uso de herramientas automáticas (licenciadas y de uso libre como las que utilizan los hackers), alineándose con estándares internacionales aceptados para la práctica de pruebas de penetración como OSSTMM, CVSS y OWASP.

El análisis de vulnerabilidades cuenta con un catálogo de nivel de exposición de la vulnerabilidad frente a la amenaza cibernética.

5 (Crítico): Vulnerabilidades cuya explotación exitosa puede comprometer un sistema.

4 (Alto): Vulnerabilidades cuya explotación exitosa puede otorgar privilegios a un atacante sobre el sistema.

3 (Medio): Vulnerabilidades cuya explotación exitosa precisa combinarse con otros ataques y posiblemente elevar el nivel de exposición a Alto o Crítico.

Como resultado de las pruebas realizadas sobre la infraestructura evaluada, es posible concluir que existe un nivel de exposición Medio en las vulnerabilidades identificadas en la infraestructura tecnológica de la Agencia Nacional de Minería.

Basados en lo anterior, es importante considerer que en el año 2021 se debe continuar con ahínco, la aplicación de los planes de remediación para el cierre de vulnerabilidades e identificación de la infraestructura obsoleta teniendo en cuenta además:

a. Establecer un modelo de programación y configuración segura en la infraestructura tecnológica.

b. Bloquear el acceso a variables, librerías y hojas de estilos, a través de la configuración de reglas de filtrado de contenido.

c. Validar la configuración y nivel de cifrado de todas las comunicaciones.

d. Configurar el servidor web para utilizar autenticación HTTPS.

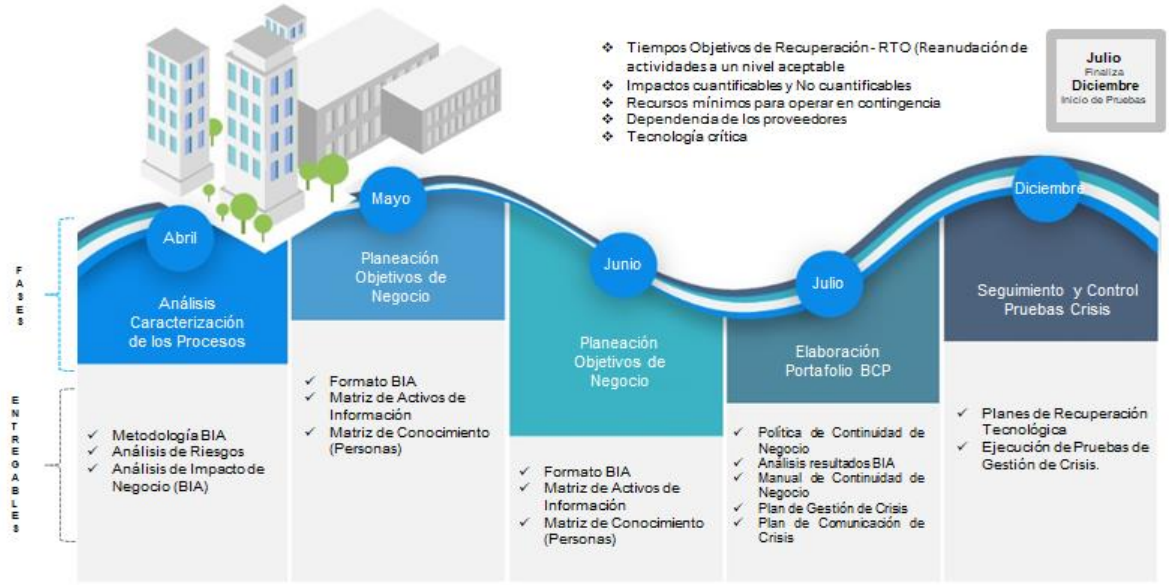
e. Configurar el sitio Web, para evitar accesos no autorizados a los archivos aplicaciones y directorios.

f. Instalar la última versión estable de los programas para evitar el uso de software con debilidades.

Esta actividad permite verificar la efectividad de las políticas de seguridad informática que existen actualmente en la Entidad y están directamente relacionados con los procesos y funcionamiento de los objetivos evaluados.

6.9. Continuidad de Negocio

La Agencia Nacional de Minería, consciente de la importancia, para que sus procesos sean cada vez más Resilientes ante las amenazas adversas e inminentes del ciberespacio y, que, dentro de su ruta de iniciativas para garantizar la seguridad y la continuidad de sus operaciones, ha identificado de manera relevante estas iniciativas que se enmarcan a continuación.



Fuente: Imagen original de la ANM (Capacidades Resilientes Continuidad de Negocio)

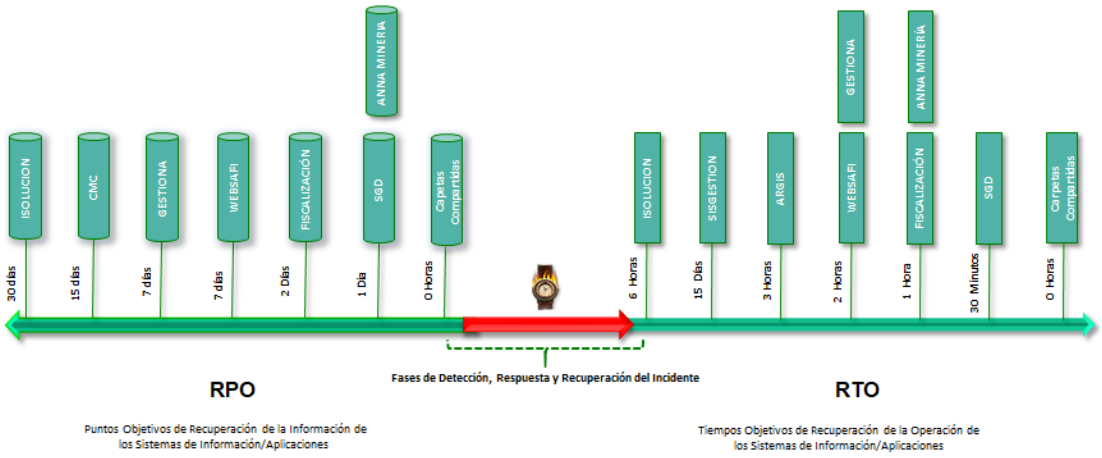
El Plan de Continuidad de Negocio en la Agencia Nacional de Minería, contempla un conjunto de iniciativas predeterminadas para reducir en un mínimo, el proceso de toma de decisiones durante momentos catastróficos o de crisis, restablecer rápidamente los procesos críticos y permitir la continuidad de la operación normal del servicio en el menor tiempo posible, teniendo como premisa la utilización de los recursos de (tecnología, personas e información), de la manera más eficiente en términos de costos.

Diseñar el Plan de Continuidad de Negocio en la Agencia Nacional de Minería, ha sido un reto ambicioso, que ha permitido contar con los recursos específicos de cada uno de los procesos críticos para la Entidad, razonables para recuperar la operación ante un desastre inexperado.

En el año 2021, se debe continuar con la revisión de la documentación que tiene como alcance la Continuidad de Negocio, que permita integrar la información de los Planes de Recuperación de cada uno de los procesos a esta documentación, vital para la continuidad de la operación en la Entidad.

1. Plan Gestión de Crisis
2. Metodología y Análisis BIA
3. Informe BIA
5. Consolidado Procesos Críticos BIA
6. Política de Continuidad de Negocio
7. Análisis GAP BCP

a. Delimitación de procesos o actividades críticas
b. Planes de recuperación que cubren las necesidades de negocio
c. Cubrimiento total de las áreas de la Entidad para implementar los planes de continuidad
d. Priorización en el desarrollo de proyectos en materia de continuidad de negocio
e. Un mayor conocimiento de los procesos de negocio, que contribuye a la mejora continua
f. Diseño de servicios Resilientes a interrupciones del negocio



Fuente: Imagen original de la ANM (BIA)

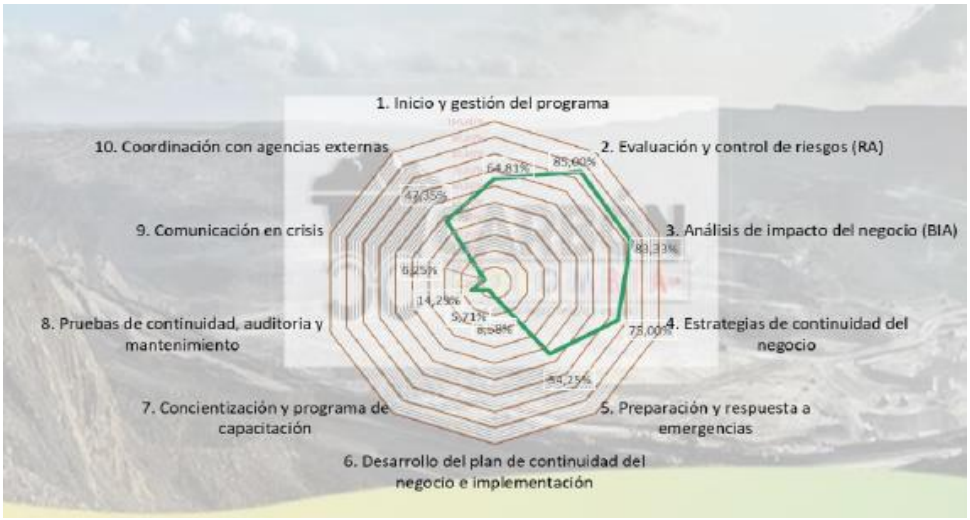
La Agencia Nacional de Minería, materialize en el año 2020, un proyecto de Hiperconvergencia para las plataformas críticas de la Entidad, estos nodos establecidos permiten tener un plan de recuperación de desastres tecnológico en tiempos óptimos para las plataformas críticas que se establecen en la imagen.

Para el año 2021, se validará además la infraestructura cesante, con el fin de poder establecer un plan de recuperación de desastres tecnológico para la infraestructura que no haga parte de hiperconvergencia.

Dentro del análisis GAP que se realizó para la Continuidad de Negocio en la Agencia Nacional de Minería, arrojó un nivel de madurez de 44,46%, antes de la implementación de la infraestructura de Hiperconvergencia.

Esta tecnología adquirida, permite esquemas de replicación que dan cumplimiento a las expectativas de los tiempos de retorno objetivo planteados por los dueños de proceso críticos de la Entidad.

Es decir que una vez llevado acabo la migración de las aplicaciones de mayor criticidad, el nivel de resiliencia de la Agencia Nacional de Minería, ha logrado un gran nivel de aceptación, debido a la implementación de los dos nodos como Centro Alterno de Datos y, como Centro de Datos de Principal.



Fuente: Imagen original de la ANM (GAP CN)

Estrategias para otros Escenarios de Disrupción.

a. Falta de Recurso Humano

- ✓ Planes de sucesión internos en los procesos de la Entidad.
- ✓ Planes de intercambio de personas entre grupos con funciones afines.
- ✓ Convenio inter-institucional con otras entidades del sector minero energético como parte de la resiliencia en la continuidad de las operaciones.

b. Falta de Proveedor Crítico

- ✓ Exigir contractualmente y con nivel de acuerdo de servicio al proveedor critico plan de continuidad del servicio tercerizado.
- ✓ Alta disponibilidad.

c. Afectación Eventos Naturales o Pandemia

- ✓ Trabajo en Casa y/o Teletrabajo excepto visitas de Fiscalización, Salvamento Minero.

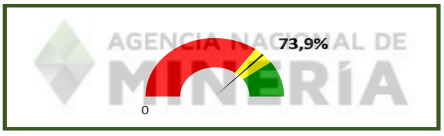
7. Medición del Modelo de Seguridad y Privacidad de la Información

La medición se realiza con un indicador de gestión que está orientada principalmente a la eficacia y eficiencia de los componentes de implementación y gestión definidos en el modelo de la operación del sistema de seguridad y privacidad de la información y ciberseguridad.

Indicador que se alimenta de la información y evidencias obtenidas desde el Sistema de Gestión de Seguridad de la Información y que permiten adoptar nuevas decisiones y estrategias en los controles de seguridad, definidos en el Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información y Ciberseguridad.

Ejemplo de uno de los indicadores que serán establecidos:

Análisis	Unid	Numero Vulnerabilidades	Vulnerabilidades Tratadas	Cerradas	KPI	W KPI
		NVD	NVT			
Indicador Tratamiento de Vulnerabilidades TIC	No.	879	650	1	73,9%	100,0%



8. Cronograma de Actividades

AGENCIA NACIONAL DE MINERÍA

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD
CRONOGRAMA DE ACTIVIDADES AÑO 2021

		CATEGORÍA / ACTIVIDAD	RESPONSABLE	FECHA DE INICIO	FECHA DE FINAL	ENTREGABLE
1		POLÍTICA, OBJETIVOS Y ALCANCE DEL SGSI	OTI	1/7/2021	30/11/2021	ENTREGABLE
	1.2	Fortalecer la Política de Continuidad de Negocio	OTI	1/7/2021	30/11/2021	Documento Word
	1.3	Fortalecer Metodología BIA y (Matriz de Impacto de Negocio)	OTI	1/7/2021	30/11/2021	Documento Word
	1.4	Fortalecer Manual de Organización de la Seguridad de la Información	OTI	1/4/2021	30/6/2021	Documento Word
	1.5	Documentar Acciones en la Declaración de Aplicabilidad - SOA	OTI	1/2/2021	30/6/2021	Documento Word
	1.7	Gestionar Matriz de Cumplimiento (MSPI y GOBIERNO DIGITAL)	OTI	1/2/2021	30/11/2021	Matriz Excel
2		MANUAL DE SEGURIDAD DE LA INFORMACIÓN	OTI	1/2/2021	31/12/2021	ENTREGABLE
	2.1	Socializar la Política de Seguridad de la Información	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
	2.2	Socializar la Política Uso Aceptable de Activos	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
	2.3	Socializar la Política de Escritorio y Pantalla Limpia	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
	2.4	Socializar la Política Transferencia de Información	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
	2.5	Socializar la Política para Dispositivos Móviles	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
	2.6	Socializar la Política de Uso e Instalación de Software Operacional	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia

SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD
CRONOGRAMA DE ACTIVIDADES AÑO 2021

CATEGORÍA / ACTIVIDAD				RESPONSABLE	FECHA DE INICIO	FECHA DE FINAL	ENTREGABLE
		2.7	Socializar la Política de Controles Criptográficos	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
		2.8	Socializar la Política de Seguridad de las Comunicaciones	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
		2.9	Socializar la Política de Desarrollo Seguro de Sistemas de Información	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
		2.10	Soocializar la Política Servicios en la Nube	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
		2.11	Socializar la Política de Teletrabajo	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
		2.12	Socializar la Política Seguridad Física y del Entorno	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
		2.13	Socializar la Política en la Relación con los Proveedores	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
	3	GESTIÓN DE LOS DOMINIOS DEL SGSI		OTI	1/2/2021	31/12/2021	ENTREGABLE
		3.1	Gestión Identificación de Activos de Información	OTI	1/2/2021	31/12/2021	Matriz de Activos
		3.2	Gestión Identificación de Riesgos de Seguridad y Ciberseguridad	OTI	1/2/2021	31/12/2021	Matriz de Riesgos
		3.3	Gestión Implementación de Planes de Tratamiento Riesgos	OTI	1/2/2021	31/12/2021	Informe de Implementación
		3.4	Gestión Plan de Recuperación de Desastres - DRP	OTI	1/2/2021	31/12/2021	Documento Word
		3.5	Gestión Planes de Continuidad de Negocio - BCP	OTI	1/2/2021	31/12/2021	Documento Word
		3.6	Gestión Plan de Pruebas de Continuidad de Negocio	OTI	1/2/2021	31/12/2021	Documento Word
		3.7	Gestión Visitas a Proveedores Críticos	OTI	1/2/2021	31/12/2021	Matriz Evaluación Proveedores
		3.8	Gestión Remediación de Vulnerabilidades	OTI	1/2/2021	31/12/2021	Matriz de Vulnerabilidades
		3.9	Gestión Incidentes de Seguridad de la Información	OTI	1/2/2021	31/12/2021	Informe del SOC
		3.10	Gestión Campañas de Concienciación - Foro	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
		3.11	Gestión Pruebas de Ingeniería Social	OTI	1/2/2021	31/12/2021	Informe de Resultados
		3.12	Gestión Capacitaciones en Seguridad y Ciberseguridad	OTI	1/2/2021	31/12/2021	Presentación - Lista Asistencia
		3.13	Gestión de la Configuración - CMDB	OTI	1/2/2021	31/12/2021	Informe Herramienta
		3.14	Gestión de Accesos Privilegiados - CyberArk	OTI	1/2/2021	31/12/2021	Informe Herramienta
	4	REVISIÓN Y ACTUALIZACIÓN DE DOCUMENTOS DEL SGSI Y SGCN		OTI	1/2/2021	31/12/2021	ENTREGABLE
		4.1	Procedimiento de Respuesta a Incidentes	OTI	1/2/2021	31/12/2021	Documento Word
		4.2	Procedimiento de Activos de Información	OTI	1/2/2021	31/12/2021	Documento Word
		4.3	Procedimiento de Vulnerabilidades	OTI	1/2/2021	31/12/2021	Documento Word
		4.4	Procedimiento de Intercambio de Información	OTI	1/2/2021	31/12/2021	Documento Word
		4.5	Procedimiento de Borrado Seguro	OTI	1/2/2021	31/12/2021	Documento Word
		4.6	Procedimiento de Evidencia Digital	OTI	1/2/2021	31/12/2021	Documento Word
		4.7	Procedimiento de relación con Proveedores	OTI	1/2/2021	31/12/2021	Documento Word
		4.8	Procedimiento de Derecho de Propiedad Intelectual	OTI	1/2/2021	31/12/2021	Documento Word
		4.9	Procedimiento Dar de Baja un Software	OTI	1/2/2021	31/12/2021	Documento Word
		4.10	Procedimiento De la Configuración	OTI	1/2/2021	31/12/2021	Documento Word
		4.11	Procedimiento de la Capacidad	OTI	1/2/2021	31/12/2021	Documento Word
		4.12	Procedimiento de Copias de Respaldo y Restauración	OTI	1/2/2021	31/12/2021	Documento Word
		4.13	Instructivo de Seguridad de Cifrado	OTI	1/2/2021	31/12/2021	Documento Word
		4.14	Instructivo de Copias de Respaldo y Restauración	OTI	1/2/2021	31/12/2021	Documento Word
		4.15	Manual de Adquisición, Mantenimiento y Desarrollo de Sistemas	OTI	1/2/2021	31/12/2021	Documento Word
		4.16	Metodología Declaración de Aplicabilidad - SOA	OTI	1/2/2021	31/12/2021	Documento Word
		4.17	Manual Organización de la Seguridad de la Información	OTI	1/2/2021	31/12/2021	Documento Word
		4.18	Análisis de Impacto de Negocio - BIA	OTI	1/2/2021	31/12/2021	Documento Word
		4.19	Manual Continuidad de Negocio	OTI	1/2/2021	31/12/2021	Documento Word
		4.20	Plan de Comunicación de Crisis	OTI	1/2/2021	31/12/2021	Documento Word
		4.21	Plan de Pruebas de Continuidad de Negocio	OTI	1/2/2021	31/12/2021	Documento Word

9. Conclusiones

a. Es necesario dar continuidad al trabajo que se viene realizando frente a la Seguridad y Privacidad de la información y Ciberseguridad de la ANM, alcanzado hitos importantes para fortalecer la protección de la información frente a las amenazas del ciberespacio.

b. Involucrar a los dueños de los procesos, quienes deben tomar conciencia en cuanto a la debida diligencia frente a la gestión de riesgos y de los controles requeridos para proteger la información de los procesos.

c. La capacitación y concienciación de los funcionarios y dueños de los procesos es uno de los frentes que se debe trabajar con prioridad. Sin la motivación y participación activa de todos los involucrados, no se logrará los objetivos en la implementación del Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

d. Se debe dejar en contexto que la Seguridad y Privacidad de la información y la Ciberseguridad, es responsabilidad de toda la Entidad.

e. El Plan de Continuidad del Negocio, debe estar basado en las consideraciones dispuestas desde un análisis de impacto al negocio y de riesgos de disrupción, con el fin de facilitar las estrategias de contención y recuperación para mejorar la resiliencia cibernética de la ANM.

f. Riesgos Por Disponibilidad

La Oficina de Tecnología e Información, actualmente cuenta con un Plan de Continuidad de Negocio basado en infraestructura de **Hiperconvergencia.**

g. Riesgos Por Confidencialidad

La Oficina de Tecnología e Información ha adquirido un nuevo licenciamiento que permite mayor seguridad a través de las herramientas colaborativas y de Nube. Entre éstas están:

a. Segmentos de navegación a través de internet para una mejor navegación segura.

b. La autenticación para los accesos (credenciales) por VPN se ha direccionado hacia el Directorio Activo, lo cual permite una óptima y eficaz gestión con éstas conexiones.

c. La aplicación de certificados SSL para las plataformas Web de la Entidad.

h. Riesgos Por Integridad

La Entidad cuenta con Firma digital a través de una API especialmente usada para algunos documentos del SGD.

i. Control de Acceso

La Oficina de Tecnología e Información viene adelantando acciones para contar con una confidencialidad al acceder a los sistemas de información, mediante:

a. **Doble Factor de Autenticación**
Websafi
Gestor de Contraseñas

b. **Re-CAPTCHA**
Sisgestión
Trámites en Línea
SGD - se desarrolla actualmente

Anexo 1 Control de Cambios

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