Acceso: Reservado ( ), Público (X), Clasificada ( ).

Título:

Seguimiento Plan de Seguridad y Privacidad de la Información – Segundo Trimestre 2024

Elaboró:

Secretaría General - Grupo de Tecnologías de la Información y las Comunicaciones (GTIC)

Leidy Paola Galindo Acevedo
Oscar Sanchez Sanchez
Andres Camilo Molano Mendieta

Entidad:

Ministerio de Minas y Energía

Bogotá, 18 de julio de 2024

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Energía

Contenido

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

1. PROCESO

Gestión tecnológica.

2. RESPONSABLE DEL PROCESO

Grupo de Tecnologías de la Información y las Comunicaciones
Ing. Leidy Paola Galindo Acevedo
Coordinadora Grupo TIC
Email: lpgalindo@minenergia.gov.co
Teléfono: (+57) 6012200300 Ext. 2408

3. DESCRIPCIÓN INFORME

El Plan de Seguridad y Privacidad de la Información, es el resultado de un diagnóstico y planeación para el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), conforme la evolución y actualización de las tecnologías de la información y comunicaciones (TIC). También se mejoraron las políticas, procedimientos y guías que permitieron al Ministerio de Minas y Energía MINENERGÍA, cumplir los requerimientos del Modelo de Seguridad y Privacidad de la información (MSPI) buscando la mejora continua.

El Plan de Seguridad y Privacidad de la Información, contiene los lineamientos del Modelo de Seguridad y Privacidad de la MSPI versión 3.0.2 definido por Ministerio de Tecnologías de la Información y Comunicaciones en adelante MINTIC, el cual orienta a las entidades del estado colombiano en la preservación de la confidencialidad, integridad y disponibilidad de la información, además permite fijar los criterios para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

Para la elaboración de este documento, se toma como referencia además de los lineamientos de MINTIC en el MSPI y sus correspondientes guías de apoyo, las normas ISO/IEC 27001:2022, ISO/IEC 22301:2019 e ISO/IEC 31000:2018.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

4. PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN

4.1 Gestión de Activos de Información

En cuanto a la Gestión de Activos de Información, se trazó un plan para la revisión y actualización anual de los mismos, en el primer trimestre del año en curso, se adelantó una revisión de la plantilla de inventarios, en la cual se implementan mejoras para facilitar la experiencia de los usuarios de las áreas propietarias y/o los responsables delegados para la identificación de los activos de información, durante el segundo trimestre se realizó la inclusión de información de la nueva categorización implementada en el nuevo mapa de procesos, actualización de TRD con el fin de enviar a revisión directiva y proceder a la recolección y divulgación que permita a las dependencias nutrir dicho proceso. (Para más información del documento-matriz de gestión de activos de información final, remitirse al responsable de seguridad de la información a cargo)

En este mismo sentido, se actualiza el material y se brinda apoyo a la capacitación de orientación a los usuarios en el ejercicio, con el fin de garantizar la efectividad del proceso, incentivando la importancia de la transferencia de conocimiento desde la identificación de los roles y responsabilidades en el cumplimiento del Plan de Seguridad y Privacidad de la Información al interior de grupos de trabajo.

4.2 Gestión de Riesgos de Seguridad de la Información

La gestión de riesgos de seguridad de la información desempeña un papel crucial para el Ministerio de Minas y Energía al enfrentar los desafíos y oportunidades en un entorno digital dinámico y cada vez más complejo. Al identificar, evaluar y mitigar los riesgos de seguridad de la información, el Ministerio no solo protege los activos críticos de datos y sistemas, sino que también salvaguarda la confianza pública y fortalece su capacidad para cumplir con las obligaciones regulatorias. Además, una gestión efectiva de riesgos proporciona una base sólida para la toma de decisiones informadas, promoviendo la continuidad operativa y minimizando el impacto de posibles incidentes de seguridad.

Teniendo en cuenta lo anterior y haciendo cumplimento del cronograma periódico que se estableció en plan de seguridad y privacidad de la información se tienen los siguientes resultados:

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

A. Ejecución de análisis de riesgos de seguridad:

Teniendo en cuenta la categorización de cada uno de los riesgos se establecieron y ejecutaron las siguientes pruebas con el fin de obtener resultados que sirvan como insumo para el análisis y tratamiento de estos:

Riesgos de Gestión:

- Verificación manual en sitio mes de mayo y junio:

  Para la actividad de extracción de la evidencia fotográfica de los equipos, se realiza de manera aleatoria al momento en el que el usuario final genera una solicitud de servicio en el aplicativo Aranda o vía correo electrónico, el técnico de mesa de ayuda realiza la intervención del equipo y procede con la toma de pantallazos

  Para el segundo trimestre se hace 2 veces el proceso teniendo como resultado la siguiente información:

MES	RESULTADO
ABRIL	⚡ De acuerdo con el diagnosticó de los diez (10) equipos intervenidos se puede entregar como resultado que no se encuentra software no autorizado instalado en los mismos. ⚡ El Ministerio de Minas y Energía posee herramientas que facilitan el cumplimiento de las directrices impartidas por la Dirección Nacional de Derecho de Autor. (*Aranda, Kaspersky)* ⚡ El Ministerio de Minas y Energía cuenta con el parque tecnológico totalmente libre de software no autorizado instalado o ilegal.
MAYO	⚡ De acuerdo con el diagnosticó de los diez (13) equipos intervenidos se puede entregar como resultado que no se encuentra software no autorizado instalado en los mismos. ⚡ El Ministerio de Minas y Energía posee herramientas que facilitan el cumplimiento de las directrices impartidas por la Dirección Nacional de Derecho de Autor. (*Aranda, Kaspersky)* ⚡ El Ministerio de Minas y Energía cuenta con el parque tecnológico totalmente libre de software no autorizado instalado o ilegal.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

JUNIO	⚡ De acuerdo con el diagnosticó de los diez (12) equipos intervenidos se puede entregar como resultado que no se encuentra software no autorizado instalado en los mismos. ⚡ El Ministerio de Minas y Energía posee herramientas que facilitan el cumplimiento de las directrices impartidas por la Dirección Nacional de Derecho de Autor. (*Aranda, Kaspersky)* ⚡ El Ministerio de Minas y Energía cuenta con el parque tecnológico totalmente libre de software no autorizado instalado o ilegal.

Reportes trimestrales de vencimientos de licenciamiento de software y de elementos de hardware dados de baja - Solicitud de elementos a renovar - Cronograma de mantenimiento - Reportes de ejecución del cronograma de mantenimiento:

Se realiza el mantenimiento preventivo de equipos de oficina, servidores y unidades de almacenamiento del Ministerio de Minas y Energía. Los equipos están ubicados en la sede principal del ministerio en la calle 43 N°57-31 CAN y en la sede del Archivo en la Carrera 50 N°26 – 20, Bogotá., se intervinieron **207 equipos en el mes de junio 2024.**

El mantenimiento preventivo de equipos es importante para asegurar el óptimo funcionamiento y prolongar la vida útil de los dispositivos tecnológicos. Este procedimiento detalla las actividades y pasos necesarios para realizar de manera efectiva el mantenimiento preventivo de equipos ofimáticos, asegurando que se cumplan los estándares de rendimiento y fiabilidad establecidos.

Durante la intervención, se realizan las siguientes tareas:

- Se realiza una limpieza física externa completa del equipo.
- Se limpian los periféricos asociados. -
- Se efectúa un soplado interno de la CPU *(excepto en portátiles y equipos AIO).*
- Se valida el estado de las partes internas.
- Se ajustan las partes internas si es necesario.
- Se colocan stickers según corresponda.
- Se verifica el estado del equipo encendiéndolo.
- Se revisa el funcionamiento del software instalado en el equipo.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Los procesos y hallazgos encontrados durante este mantenimiento se encuentran en el informe de mantenimiento preventivo junio 2024 presentado por la empresa B2B Tic, si se requiere más información gestionarla con el responsable de seguridad de la información a cargo.

- Informe de capacidad y actualización de software de ciberseguridad enfocados en la defensa y monitoreo de los sistemas de infraestructura y sistemas de información; WAF, FAZ, FW, VPN, afinamiento Firewall y antivirus:

1. **Afinamiento de Fortigate FW :**

   El Equipo Fortigate maestro del ministerio de minas y energía en la actualidad está operando normalmente, **presenta consumo de Memoria en 39 % y CPU 4%**; en datos registrados en la consola web que visualizan gráficamente su conducta, pretendiendo describir brevemente el comportamiento, funcionamiento y disponibilidad apremiando la toma de decisiones de acuerdo con los resultados obtenidos en el lapso del segundo trimestre del año 2024.

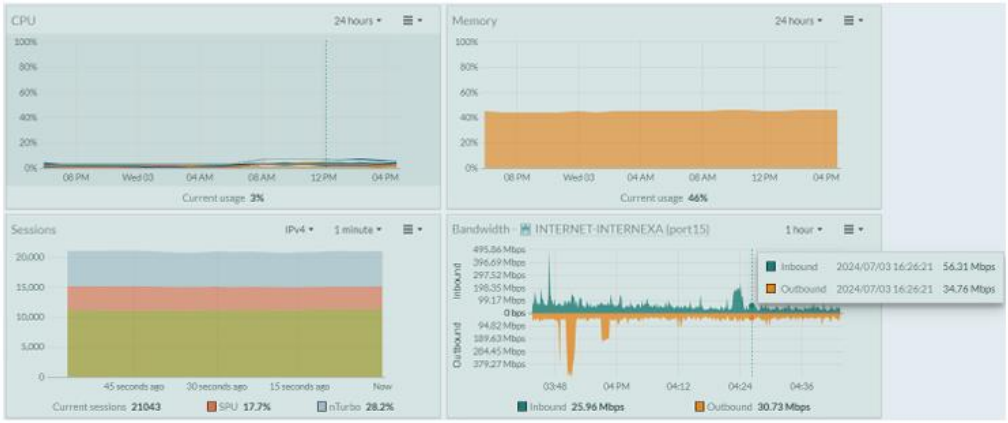


Imagen 1. Ejemplo de trafico de consumo de red y de recursos por FW.

El equipo se encuentra licenciado hasta diciembre del 2026- actualizado en mayo del 2024 (HA activo) , con todas sus características de fortiguard, soporte y garantía:

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Imagen 2. Estatus de licenciamiento de las herramientas de monitoreo y defensa

Durante el afinamiento se realizaron los siguientes procesos:

a. **Estado HA Cluster:** Se realiza verificación del estado del HA Cluster ACTIVO-PASIVO el cual se determina que el equipo master es XXXX_FW_1 con una prioridad de 200 y el equipo slave es XXXXXS2 con una prioridad de 150, en estado de buen funcionamiento.

b. **Configuración Logs Equipo:** El Fortigate se encuentra configurado para almacenar logs en un FortiAnalyzer, esto permite que podamos almacenar logs para tener trazabilidad de los eventos y adicionalmente poder generar reportes de tráfico.

c. **Configuración Agente FSSO:** Se verifica que el equipo está haciendo uso del agente FSSO con estado funcional, esto permite identificar los usuarios para configurar los permisos de navegación.

d. **Consumo de canal de datos:** Se realiza la revisión del consumo del canal evidenciando que no hay saturación de canales o interfaces

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Imagen 3. Gráfico de consumo de datos del FW , pruebas tomadas en ciclo de vida activo

e. **Afinamiento de políticas en el WAF:** Se deshabilita la opción de monitor mode con el fin de empezar a aplicar los filtros de seguridad en cada una de las políticas, además, se configura perfil de protect hostname y web protection profile a las políticas activas que no lo estaban usando con el fin de protegerlas ante accesos y ataques que puedan surgir a nivel web, adicionalmente, se eliminan usuarios locales en el firewall que ya no se utilizan y se desactivan otros ya que se identifica no tienen contrato vigente

f. **Revisión de políticas hacia zona DMZ:** Se configuran políticas limitando acceso y puertos desde VPN y LAN hacia DMZ haciendo énfasis en los permisos hacia las herramientas de administración.

g. **Bloqueo de amenazas - IP de origen:** Se configura bloqueo de IPs que han generado algún tipo de intento de ataque al Minenergia

h. **Revisión de HA:** Se deshabilita puertos y de generan nuevas conexiones para máxima escalabilidad del FW.

i. Cambio de equipo Fortiweb por inconveniente a nivel físico.

j. Se actualizan firmware de equipos Firewall y Fortianalizer.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Teniendo en cuenta los numerales anteriores y si se desea saber más información a detalle del afinamiento de los equipos de ciberseguridad que se encuentra en la infraestructura del Minenergia, puede contactarse con el responsable de seguridad de la información a cargo en el Grupo de Tecnologías de la Información y las Comunicaciones.

2. **Conexiones de VPN FortiClient:**

Teniendo cuenta los lineamientos del MPSI y el control de acceso que se tiene identificado en la normatividad ISO27001 se hace una revisión de los usuarios que usan la conexión de remota para acceder a la red del Minenergia mediante la VPN y su sistema de seguridad evidenciado en la herramienta de FortiClient, a continuación, se muestra las características del monitoreo:

VPN Logins MME - Trimestre 2 - 2024

#	Usuario	Type	First Used	Total Number of Connections	Total Duration Connected(HH:MM:SS)

Imagen 4. Características identificadas y sectorizadas del análisis de login de la VPN

Si se desea saber el listado completo de monitoreo y su actividad, puede remitirse al responsable de seguridad de la información a cargo en el Grupo Tic.

3. **Disponibilidad de FW, WAF Y FAZ:**

Es importante determinar más allá del monitoreo de las herramientas (información objetivo), establecer el tiempo de ejecución y aplicación de estas, es por esto, que, según los lineamientos de la gestión de riesgos de seguridad y privacidad de la información, los sistemas de defensa deben estar en constante funcionamiento (sin interrupciones), ya que estos tiempos de no disponibilidad pueden ser brechas para un ataque de día cero.

Dicho lo anterior se tiene la siguiente estructura de monitoreo de disponibilidad:

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

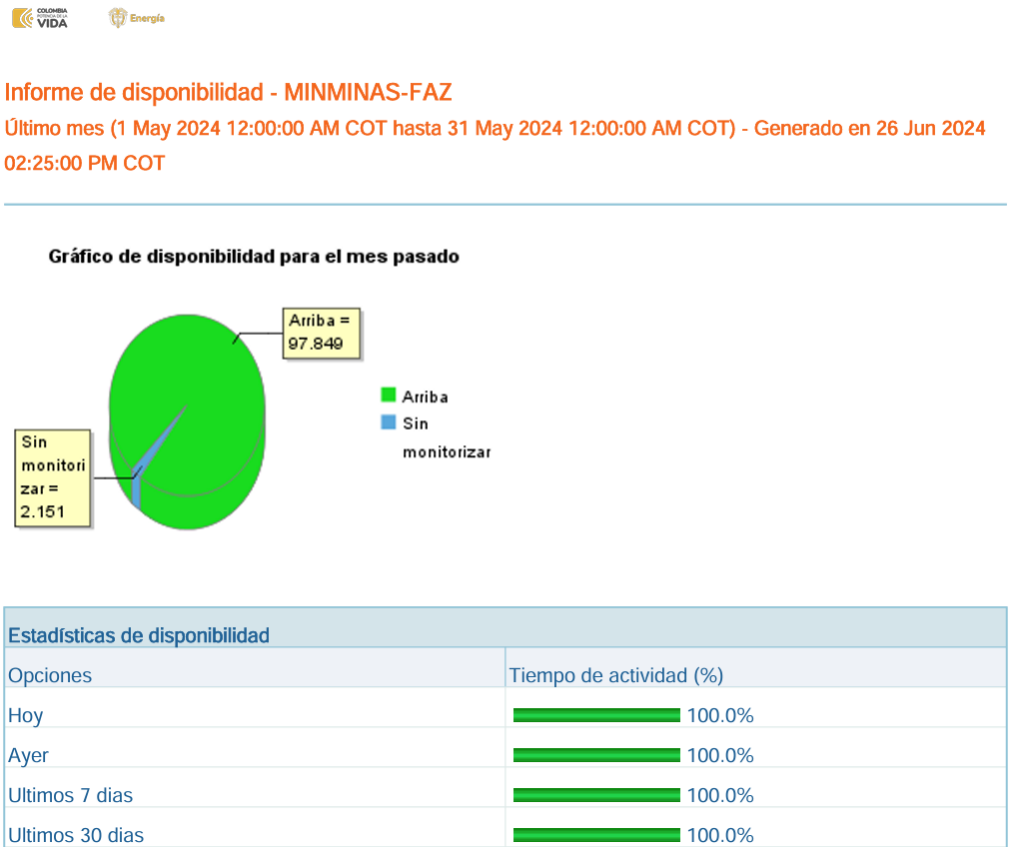


Imagen 5. Ejemplo de visualización grafica de disponibilidad de recursos

Dicha estructura establece tiempos de disponibilidad por intervalos predefinidos (frecuencia de escaneo) por cada una de las herramientas, los resultados identificados para el segundo trimestre del año 2024 es que existe una disponibilidad 24/7 (cumplimiento del 98%) con una franja de monitorización (no necesariamente indisponibilidad) del 2% en falla, para mayor detalle puede consultar al responsable de seguridad de la información a cargo.

4. **Informe y seguimiento de ejecución del antivirus:**

En conformidad y alineados a la normatividad ISO27001 se ejecuta un informe mensual con el proveedor y la herramienta de seguridad (**última actualización 14.2.0.29967**), dicho software es el encargado de analizar, monitorear y defender la infraestructura de los SI que actualmente tiene el Minenergia.

Destacando los siguientes ítems:

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

a. Claves de licencia
b. Distribución de la protección
c. Bases de datos de antivirus.
d. Estado de protección.
e. Informe de amenazas vigentes.
f. Dispositivos más afectados.
g. Informe de despliegue.
h. Informe de vulnerabilidades identificadas.
i. Control web.
j. Estado de los servidores

Dentro de los hallazgos determinados por este informe (ultima evaluación hecha en el mes de mayo) más relevantes se tiene lo siguiente:

1. **Licenciamiento:** Se tienen 1200 licencias adquiridas, 625 en uso y 575 disponibles.

2. **Base de datos de malwares:** las bases de datos están actualizadas.

3. **Estado de protección:**

    - Se ha perdido la conexión con el dispositivo: # dispositivos
    - La aplicación de seguridad no está instalada: # dispositivos
    - Se ha perdido la conexión con el dispositivo.
    - La protección esta desactivada: 0 dispositivos
    - Se ha perdido la conexión con el dispositivo. El dispositivo no tiene espacio disponible en el disco: # dispositivo
    - Las bases de datos están desactualizadas: # dispositivo

    Para más información sobre el # de dispositivos remitirse al responsable de seguridad de la información a cargo.

4. **Informe de amenazas:**

    Intrusión de 2 ataques: los cuales fueron identificados y eliminados (ataque diseñado para robo de información y tomar control de cámaras web, SI, y pulsaciones de teclas) para más información dirigirse al responsable de seguridad de la información a cargo en el Grupo Tic.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

5. **Dispositivos infectados:**

   Se tiene identificado posibles dispositivos infectados, de manera que se debe realizar el proceso a seguir para la limpieza y extracción del malware, para más información dirigirse al responsable de seguridad de la información a cargo en el Grupo Tic.

6. **Validación del estado de los servidores:**

   Hay novedades descritas y encontradas en el proceso de análisis de los servidores, los procesos de seguridad de la información deben ejecutarse para evitar posibles vulnerabilidades en el futuro, para más información detallada se debe remitir al responsable de seguridad de la información a cargo.

   Informes de operación y disponibilidad de canales con los diferentes operadores de telecomunicaciones de los meses de abril, mayo y junio:

   El Informe de gestión mensual contiene información relevante para evidenciar el nivel de cumplimiento del acuerdo firmado entre el Ministerio de Minas y Energía y el operador, presenta los resultados y el análisis de la gestión de los servicios para los meses correspondientes al segundo trimestre del año 2024 discriminados entre sí, presenta el nivel de cumplimiento de los servicios contratados y relaciona los resultados y el análisis de la gestión del servicio para el periodo en referencia.

   A partir de dicha información los SLA's contratados por el Minenergia evalúan un desempeño optimo con cumplimiento del **100% de la operación sin novedad de eventos** durante los meses descritos, para más información y detalle de características técnicas (velocidad, picos de consumo y/o eventos relacionados) comunicarse con el responsable de seguridad de la información a cargo en el Grupo Tic.

Riesgos de Seguridad y Privacidad de la Información

- Reportes Segundo Trimestre de identificación de lenguajes de programación o aprobación de cambios en la metodología o publicación de versión final de metodología o sensibilización en los ajustes realizados

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Acorde a los lineamientos del MSPI y la normatividad de código seguro que se debe implementar en desarrollo de software, se finaliza en el segundo trimestre del 2024 el documento de ***"Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información y Nuevas Aplicaciones del Ministerio De Minas Y Energía"*** anexando los numerales 8 y 9; en el primero se establece el proceso de construcción seguro de software donde se determina lo siguiente:

1. Análisis de requerimientos (según necesidad y criticidad de la información).
2. Desarrollo – requerimientos y procesos con mínimos de seguridad.
3. Pruebas – Entornos de Sandbox para análisis de vulnerabilidades y riesgos.
4. Despliegue o puesta en marcha – Seguimiento de posibles vulnerabilidades de ataques de día cero.
5. Capacitación y concientización de las buenas prácticas de desarrollo.

A través de dicho proceso se estableció un "check list" de preguntas fundamentales para que el desarrollador/a al momento de evaluar el requerimiento y finalizar su responsabilidad pueda determinar si está cumpliendo con la metodología establecida, dicho documento se centra en los siguientes conceptos:

Tabla 1. Conceptos de check list de código seguro.

N°	CONCEPTO
1	Patrones de Diseño Seguros
2	Antipatrones a evitar
3	Arquitecturas Seguras
4	Prácticas de Desarrollo Seguro
5	Principio de Privilegio Mínimo
6	Ciclo de Vida de Desarrollo Seguro (SDLC)
7	Revisiones de Código y Pruebas
8	Seguridad en la Infraestructura

En el segmento número 9 se establecen según guías y normatividad internacional *"Owasp Top 10 y PCI DSS"* los riesgos más significativos que se tienen durante el desarrollo de software y sus recomendaciones para lograr los mejores resultados.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Para más información de la metodología que implementará el Minenergia para el desarrollo por favor remitirse al documento o al área encargada para su revisión.

- Informe trimestral de Auditoría a los Logs de los SI para su monitoreo y control:

  Describir el procedimiento que se trabajará para implementar módulos de auditoría (Logs - los que apliquen) en los sistemas de información que se encuentran bajo la gobernabilidad del Ministerio de Minas y Energía, teniendo en cuenta los estándares que establece lo siguiente: Se adopta la Política General de Seguridad y Privacidad de la Información, la Política de Tratamiento Y Protección de Datos Personales, la Política de Continuidad del Negocio, la Política ante Recuperación ante Desastres TIC y las Políticas de Seguridad y Privacidad de la Información.

  Para el informe del según trimestre del año 2024, se establecen los diferentes SI que están determinados bajo una caracterización de “consulta” y otros de “auditoria”, el paso siguiente es que bajo el perfilamiento del grupo TIC del Minenergia se defina si dicha caracterización es correcta para usar la herramienta de auditoria en cada uno de los procesos (necesarios) y tener resultados para su posterior análisis. Para más información de la división de estos SI, contactar al responsable de seguridad de la información a cargo en el Grupo Tic.

  El módulo de auditoría "site-history" de Wagtail es una herramienta esencial para los administradores que necesitan realizar un seguimiento de los cambios realizados dentro de su sitio web, este módulo registra una amplia variedad de acciones en el sitio, incluidas modificaciones de contenido, creaciones y eliminaciones de páginas.

  Al ofrecer una visión clara y detallada del historial de modificaciones, "site-history" es invaluable para la gestión de la seguridad, la auditoría de contenido y la resolución de problemas.

- Informes trimestrales de las actividades de respaldo generados desde ARANDA y la programación de backups.

  Para el segundo trimestre del año 2024 se presenta el informe de respaldo, donde los indicadores a destacar son:

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

RPO
Schedule (horario ejecución)
Medio de almacenamiento (Local - Cintas)
Criticidad (alto - medio - bajo)
Frecuencia o periodicidad
Tipo de copia (full - Incremental)
Retención (días)

Es importante resaltar que el nivel de backup y su frecuencia está determinado por el nivel de criticidad que tienen los sistemas de información y así mismo se debe terminar el periodo (generalizado en horas de la noche) cuando se hace la copia de seguridad y el RPO (máxima perdida de datos) que se debe tener al momento del proceso.

Para obtener el informe detallado de los SI y su frecuencia del proceso se debe contactar con el responsable de seguridad de la información a cargo en el Grupo Tic.

Dicho lo anterior y con base a los sistemas de información dateados, se genera un **backup discriminado de 122 activos de información**, que varían su frecuencia.

- Informes de las pruebas o simulacros realizados a partir del DRP:

En el segundo trimestre del 2024 (25/06/2024) se define y se registra las pruebas y procedimientos necesarios para la demostración de las capacidades de la redundancia de los fabric interconnect dispuestos en ambos datacenter en un esquema de HA (Activo - Pasivo) para el Ministerio De Minas y Energía en sus soluciones de hiper-convergencia, de manera que para esta etapa se debe realizar:

- Pruebas falla nodo fabric interconnect

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Tabla 2. Procesos indicados para las pruebas del datacenter

N°	PRUEBA
1	Validación del estado HA
2	Establecimiento de pruebas de conectividad
3	Reinicio pasivo
4	Establecimiento del HA
5	Reinicio y conmutación
6	Establecimiento del HA

Dichas pruebas se realizan tanto en el data center principal como el alterno para mitigar, analizar y determinar riesgos asegurados de la solución de infraestructura.

Para mayores detalles de los resultados de dichas pruebas contactarse con el responsable de seguridad de la información a cargo en el Grupo Tic.

- Medios y dispositivos de los usuarios cifrados y protegido.

Se están realizando pruebas con la política de cifrado del antivirus, los resultados serán confirmados cuando se establezca el procedimiento o mecanismo correcto de clave de cifrado del dispositivo con la información cifrada, versus el proceso inverso para descifrar la información.

4.3 Tratamiento de Riesgos

Dando cumplimento a la "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. Versión 6", expedida por el DAFP en noviembre de 2022 se hace este segundo informe trimestral 2024 (segundo trimestre) que conlleva el seguimiento del plan de seguridad y privacidad de la información y la gestión de riesgos TIC.

4.4 Gestión de políticas y procedimientos

En consecuencia, con la revisión efectiva de gestión de riesgos y políticas de seguridad se establece la fase 2 como cumplimiento y alineación al MSPI de MINTIC, acorde a la frecuencia que se debe realizar este tipo de procedimientos y se muestra en la tabla 3:

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Tabla 3. Gestión de Políticas y Procedimientos de Seguridad de la Información

N°	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE	FECHA
1	Revisar los incidentes del periodo anterior, los resultados del análisis de riesgos, las auditorías de seguridad, los cambios organizacionales que haya surtido la Entidad y la revisión por la dirección.	Oficial de seguridad de la información o quien haga sus veces.	Semana 4 Mes 7
2	Establecer plan de ajustes para las políticas y procedimientos de seguridad.	Oficial de seguridad de la información o quien haga sus veces.	Semana 2 mes 8
3	Inicio de los cambios necesarios a las políticas y procedimientos de seguridad.	Oficial de seguridad de la información o quien haga sus veces.	Semana 1 Mes 9
4	Aprobar las políticas de seguridad.	Comité institucional de gestión y desempeño.	Semana 1 Mes 10
5	Divulgar las políticas de seguridad.	Oficina de Planeación y Gestión Internacional.	Semana 2 Mes 10

4.5 Gestión de recursos de seguridad

Teniendo en cuenta las actividades que se debían ejecutar para poder gestionar los recursos correspondientes para el mantenimiento de seguridad de la información y haciendo un seguimiento de dicho proceso se tienen el proceso abierto frente a la infraestructura de ciberseguridad y ciberdefensa que tiene el Minenergia.

Para saber más información de los lotes y requerimientos que se está solicitando por parte del ministerio remitirse al área encargada.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

5. PLAN DE SEGUIMIENTO Y EVALUACIÓN DE LA IMPLEMENTACIÓN Y MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN

5.1 Gestión de indicadores

Los indicadores deben revisarse y actualizarse según el resultado de la revisión por la dirección en la cual se establece la información que esta requiere, para valorar la gestión realizada en el periodo anterior.

5.2 Gestión de Vulnerabilidades

Acogiendo el control de gestión de vulnerabilidades técnicas, registrado en el anexo a de la norma ISO 27001, en lo cual se debe tener en cuenta no solo la ejecución de pruebas de vulnerabilidad, sino que también su acción correctiva y verificación de que las actividades ejecutadas, se reportan en el periodo entre otras acciones:

Avance de la implementación de autogestor de contraseñas:

La transformación de la ciber amenaza con relación a las contraseñas empleadas por cambio constantemente y aun es habitual que un número considerable de personas empleen la misma para todo, cuando debería usar una diferente por cada sitio web o servicio de la información en la que se registra.

El Ministerio usó un gestor de contraseñas, que además de ahorrar tiempo al gestionar contraseñas, implementa acciones para mejorar las prácticas y fortalecer su nivel de seguridad.

Para comprobar y aprobar el cambio, los usuarios deben elegir contraseñas que cumplan con los requisitos establecidos para una contraseña segura. Una vez esta es aprobada se agregan al grupo definitivo de usuarios cuya contraseña se vencerá cada 90 días, fecha en la que se reiniciará el ciclo.

En la actualidad el plan de trabajo ha logrado la implementación de este gestor en los diferentes grupos de trabajo:

- Grupo de Tecnologías de la Información y las Comunicaciones
- Subdirección de Talento Humano
- Dirección de Hidrocarburos
- Grupo de Gestión Contractual

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Para el segundo trimestre y siguiendo la hoja de ruta se logró la implementación de dicho gestor de contraseñas para 35 grupos objetivo de acuerdo con la siguiente lista:

Tabla 4. Grupos objetivo para la implementación de gestor de contraseñas segundo trimestre 2024

N°	GRUPO OBJETIVO
1	Oficina Asesora Jurídica
2	Grupo de Coordinación Interinstitucional y Seguimiento de Fallos
3	Grupo de Energía Eléctrica
4	Grupo de Hidrocarburos
5	Grupo de Minas
6	Grupo de Defensa Judicial Y Asuntos Constitucionales
7	Oficina de Asuntos Ambientales y Sociales
8	Grupo de Gestión Ambiental
9	Oficina de Planeación y Gestión Internacional
10	Grupo de Gestión del Cumplimiento
11	Grupo de Gestión internacional
12	Grupo de Gestión y Desempeño
13	Grupo de Programación y Gestión Estratégica de Proyectos
14	Subdirección Administrativa y Financiera
15	Grupo de Comisiones de Servicio y Gastos de Desplazamiento
16	Grupo de Tesorería
17	Grupo de Gestión Administrativa
18	Grupo de Gestión Contractual
19	Grupo de Presupuesto
20	Grupo de Jurisdicción Coactiva
21	Grupo de Gestión Financiera Y Contable
22	Dirección de Formalización Minera
23	"Grupo de Coordinación Para el Fomento a la Minería Sustentable y La Seguridad Minera
24	Grupo de Coordinación Para la Formalización de actividades Mineras
25	Grupo de Coordinación Para los Programas de Minería Artesanal Y Reconversión Productiva
26	Dirección de Minería Empresarial
27	Grupo de Ejecución Y Gestión Minera

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

N°	GRUPO OBJETIVO
28	Grupo de Formulación de Política Y Reglamentación Minera
29	Grupo de Planeación Y Seguimiento Minero
30	Dirección de Hidrocarburos
31	Grupo de Gas Combustible
32	Grupo de Gestión de Proyectos y Optimización
33	Grupo Downstream
34	Grupo Midstream
35	Grupo Upstream

PORTAL CAUTIVO:

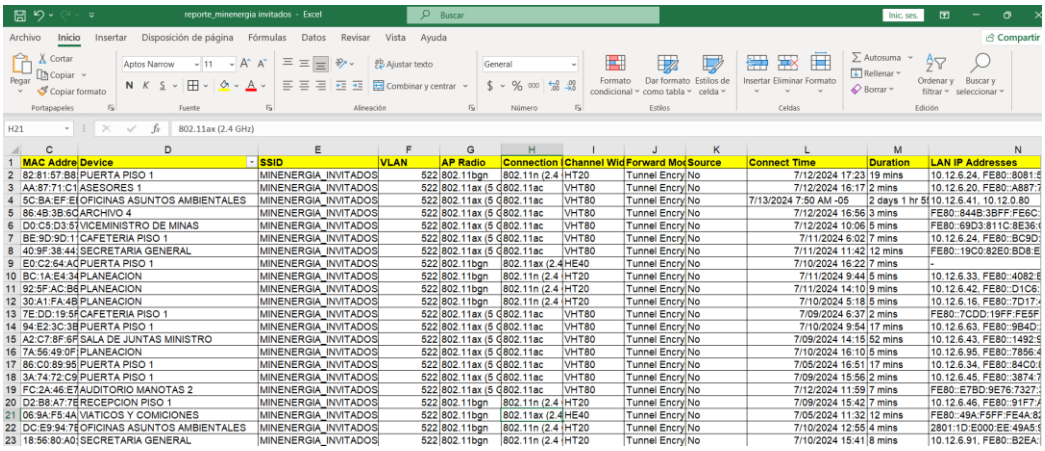
La necesidad de brindar servicios a los visitantes del Ministerio llevo a la instauración de un portal cautivo o WiFi hotspot, herramienta que permite controlar y gestionar el acceso a redes inalámbricas mediante un proceso de autenticación o registro de los visitantes del Ministerio a través de la red de WIFI MINENERGIAINVITADOS.

Estas solicitudes de registro deben ser aprobadas por los anfitriones (funcionarios o contratistas) registrados en el directorio activo y tiene entre otras políticas la restricción de navegación en páginas potencialmente peligrosas.

En el primer trimestre del año en curso 358 personas realizaron 847 conexiones, controlando quien accede a la red y evitando el uso indebido o malicioso de la misma.

Para el segundo semestre se registraron 841 conexiones en la red WIFI de visitantes a través del portal cautivo, en este periodo se realizó cambio de configuración para que esta red únicamente brinde acceso a internet a través de los puertos necesarios y no tenga conexión a la red interna, a su vez también se realizó la configuración para que estas conexiones wifi únicamente sean autorizadas desde un correo del dominio **@minenergia.gov.co.**

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300



	C	D	E	F	G	H	I	J	K	L	M	N
1	MAC Addre	Device	SSID	VLAN	AP Radio	Connection	Channel Wid	Forward Mo	Source	Connect Time	Duration	LAN IP Addresses
2	82:81:57:B8	PUERTA PISO 1	MINENERGIA_INVITADOS	522	802.11bgn	802.11n (2.4	HT20	Tunnel Encry	No	7/12/2024 17:23	19 mins	10.12.6.24, FE80::8081:5
3	AA:87:71:C1	ASESORES 1	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/12/2024 16:17	2 mins	10.12.6.20, FE80::A887:7
4	5C:BA:EF:E(	OFICINAS ASUNTOS AMBIENTALES	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/13/2024 7:50 AM -05	2 days 1 hr 5	10.12.6.41, 10.12.0.80
5	86:4B:3B:6C	ARCHIVO 4	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/12/2024 16:56	3 mins	FE80::844B:3BFF:FE6C:
6	D0:C5:D3:57	VICEMINISTRO DE MINAS	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/12/2024 10:06	5 mins	FE80::69D3:811C:8E36:(
7	BE:9D:9D:1(	CAFETERIA PISO 1	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/11/2024 6:02	7 mins	10.12.6.24, FE80::BC9D:(
8	40:9F:38:44:	SECRETARIA GENERAL	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/11/2024 11:42	12 mins	FE80::19C0:82E0:BD8:E
9	E0:C2:64:AC	PUERTA PISO 1	MINENERGIA_INVITADOS	522	802.11bgn	802.11ax (2.4	HE40	Tunnel Encry	No	7/10/2024 16:22	7 mins	-
10	BC:1A:E4:34	PLANEACION	MINENERGIA_INVITADOS	522	802.11bgn	802.11n (2.4	HT20	Tunnel Encry	No	7/11/2024 9:44	5 mins	10.12.6.33, FE80::4082:E
11	92:5F:AC:B6	PLANEACION	MINENERGIA_INVITADOS	522	802.11bgn	802.11n (2.4	HT20	Tunnel Encry	No	7/11/2024 14:10	9 mins	10.12.6.42, FE80::D1C6:
12	30:A1:FA:4B	PLANEACION	MINENERGIA_INVITADOS	522	802.11bgn	802.11n (2.4	HT20	Tunnel Encry	No	7/10/2024 5:18	5 mins	10.12.6.16, FE80::7D17:4
13	7E:DD:19:5F	CAFETERIA PISO 1	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/09/2024 6:37	2 mins	FE80::7CDD:19FF:FE5F
14	94:E2:3C:3B	PUERTA PISO 1	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/10/2024 9:54	17 mins	10.12.6.63, FE80::9B4D::
15	A2:C7:8F:6F	SALA DE JUNTAS MINISTRO	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/09/2024 14:15	52 mins	10.12.6.43, FE80::1492:9
16	7A:56:49:0F	PLANEACION	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/10/2024 16:10	5 mins	10.12.6.95, FE80::7856:4
17	86:C0:89:95	PUERTA PISO 1	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/05/2024 16:51	17 mins	10.12.6.34, FE80::84C0:8
18	3A:74:72:C9	PUERTA PISO 1	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/09/2024 15:56	2 mins	10.12.6.45, FE80::3874:7
19	FC:2A:46:E7	AUDITORIO MANOTAS 2	MINENERGIA_INVITADOS	522	802.11ax (5 G	802.11ac	VHT80	Tunnel Encry	No	7/12/2024 11:59	7 mins	FE80::E7BD:9E76:7327:3
20	D2:B8:A7:7E	RECEPCION PISO 1	MINENERGIA_INVITADOS	522	802.11bgn	802.11n (2.4	HT20	Tunnel Encry	No	7/09/2024 15:42	7 mins	10.12.6.46, FE80::91F7:4
21	06:9A:F5:4A	VIATICOS Y COMICIONES	MINENERGIA_INVITADOS	522	802.11bgn	802.11ax (2.4	HE40	Tunnel Encry	No	7/05/2024 11:32	12 mins	FE80::49A:F5FF:FE4A:8
22	DC:E9:94:7E	OFICINAS ASUNTOS AMBIENTALES	MINENERGIA_INVITADOS	522	802.11bgn	802.11n (2.4	HT20	Tunnel Encry	No	7/10/2024 12:55	4 mins	2801:1D:E000:EE:49A5:9
23	18:56:80:A0	SECRETARIA GENERAL	MINENERGIA_INVITADOS	522	802.11bgn	802.11n (2.4	HT20	Tunnel Encry	No	7/10/2024 15:41	8 mins	10.12.6.91, FE80::B2EA:4

Imagen 6 . Formato de informe del acceso al portal cautivo del Minenergia con información comprendida del segundo trimestre año 2024- ejemplo de datos, no corresponde al real

Teniendo en cuenta la imagen anterior, es importante destacar que la información del uso del portal cautivo para el segundo trimestre del año 2024 es de vital importancia para poder definir las siguientes características:

1. **Punto de conexión más usado:** Oficina de planeación
2. **VLAN de conexión**
3. **Dirección IP de acceso**
4. **MAC del dispositivo**
5. **Tiempo de conexión**

Dichas características son fundamentales como prevención y rastreo de picos de alta demanda que puede estar teniendo la red, posible investigación forense en caso de ataque desde el interior de la red, análisis de información que involucre el cambio de políticas de seguridad debido a comportamientos inesperados de los usuarios, tiempos de descongestión y posibles rutas de información alternas para tiempos de latencia menores, entre otros.

Para más información de los usuarios conectados a las distintas redes del Minenergia, debe remitirse al informe generado y que está a cargo del responsable de seguridad de la información del Grupo Tic.

5.2.1 Pruebas de ejecución de vulnerabilidades

A partir de la herramienta *Tenable* se hace la proyección y puesta en marcha de pruebas de vulnerabilidades en el segundo trimestre del año 2024, que tuvieron como

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

objetivo tener el informe detallado de las posibles brechas de seguridad de la información categorizadas de la siguiente manera:

- **Escaneo de activos**: Identificación y descubrimiento de todos los activos en la red, incluidos dispositivos, servidores, aplicaciones y servicios.

- **Detección de vulnerabilidades**: Identificación de vulnerabilidades conocidas en los activos escaneados mediante comparación con bases de datos actualizadas de vulnerabilidades.

- **Evaluación de configuraciones**: Revisión de las configuraciones de seguridad de los activos para identificar errores de configuración que podrían introducir vulnerabilidades.

- **Análisis de cumplimiento**: Verificación del cumplimiento con políticas de seguridad y estándares regulatorios mediante la evaluación de configuraciones y la presencia de vulnerabilidades específicas.

- **Escaneo de aplicaciones web**: Pruebas de seguridad de aplicaciones web para identificar vulnerabilidades como inyecciones SQL, cross-site scripting (XSS), y otros riesgos de seguridad.

- **Escaneo de contenedores y entornos de nube**: Evaluación de la seguridad en entornos de contenedores (como Docker) y plataformas en la nube para identificar configuraciones inseguras y vulnerabilidades específicas.

- **Análisis de malware y amenazas**: Detección de malware conocido y análisis de amenazas potenciales en los activos escaneados.

- **Evaluación de vulnerabilidades emergentes**: Monitoreo de nuevas vulnerabilidades que pueden ser descubiertas y actualización rápida de las bases de datos de vulnerabilidades para la detección oportuna.

Dicha caracterización anteriormente mencionada fue usada en los sistemas de información objetivo (priorización determinada a partir de la criticidad, uso y disponibilidad de la información) de la siguiente manera:

Tabla 5. Pruebas de vulnerabilidades ejecutadas segundo trimestre año 2024

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

N°	ACTIVO OBJETIVO	FECHA DE EJECUCIÓN	RESULTADO
1	Sistema SIVEEIC https://siveeic.minenergia.gov.co/#/auth/login	18/06/2024	Confidencial
2	Portal WEB del MME	13/06/2024	
3	Sistema https://www.integrame.gov.co/	25/05/2024	
4	Aplicación de Biblioteca KOHA https://biblioteca.minenergia.gov.co/	14/05/2024	
5	Aplicación web NORMATIVAME https://normativame.minenergia.gov.co/	18/06/2024	
6	Aplicación CARGAME	20/06/2024	
7	ARGO Producción https://argo.minenergia.gov.co/orfeo/login.php	8/05/2024	
8	Aplicación Model https://aulavirtualune.minenergia.gov.co/login/index.php	9/05/2024	

Considerando la información descrita, cada informe de los resultados lo remitió (mediante correo electrónico, como se muestra a continuación) el área encargada a cada dependencia correspondiente del Minenergia, para que pueda analizarse, evaluarse y mitigarse (si es necesario). El posterior seguimiento de este proceso será el paso siguiente en el tercer trimestre del año 2024 con el fin de encontrar resultados beneficiosos que conlleven a subsanar las vulnerabilidades y ser sometidas nuevamente a un re-test.

Para más información de los resultados y evidencias de comunicación de cada uno de estos procesos se debe remitir al responsable de seguridad de la información a cargo.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Imagen 8. Formato de comunicación a dependencias sobre informes de vulnerabilidades.

A partir de lo anteriormente mencionado y siguiendo los lineamientos del MSPI, el plan de seguridad de la información del Minenergia y la normatividad ISO27001 se establece el siguiente cronograma especifico que implica la ejecución de pruebas de hacking ético en activos de información objetivo para el tercer y cuarto trimestre del año 2024:

Tabla 6. Cronograma de ejecución de pruebas de vulnerabilidades, tercer y cuarto trimestre

NO	FASE	ACTIVIDAD	FECHA
1	PREPARACIÓN	Identificación de información objetivo	Mes 8 semana 2
		Definición de alcance y objetivos	Mes 8 semana 3
2	ANÁLISIS	Escaneo de vulnerabilidades (Definición y ejecución de herramienta interna o evaluación por terceros) para identificar posibles vulnerabilidades	Mes 9 semana 1
		Análisis de configuraciones (red y software)	Mes 9 semana 2
		Enumeración de servicios más expuestos	Mes 9 semana 3

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

NO	FASE	ACTIVIDAD	FECHA
3	EXPLOTACIÓN	Pruebas de pentesting (internas o por terceros), definiendo controles de acceso (caja negra, gris o blanca) según prioridad.	Mes 10 semana 1 y 2
		Análisis de impacto	Mes 10 semana 3
4	INFORME Y DOCUMENTACIÓN	Documentación de hallazgos	Mes 10 semana 4
		Recomendación de mitigación	Mes 11 semana 1
		Presentación del informe	Mes 11 semana 2
5	IMPLEMENTACIÓN	Ejecutar acciones de remediación a las vulnerabilidades detectadas.	Mes 11 semana 3
		Ejecutar pruebas de re-test para verificar que efectivamente se hayan cerrado las vulnerabilidades.	Mes 11 semana 4

5.2.2 Ventanas de mantenimiento efectuadas

A partir de los hallazgos de los sistemas de información y en alineación a la normatividad el Minenergia debe mantener sus equipos y herramientas de monitoreo actualizadas y con las últimas versiones correspondientes con el fin de poder mitigar ataques y subsanar las vulnerabilidades correspondientes, de esta manera, para el segundo trimestre del año 2024 se efectuaron las siguientes actualizaciones:

Tabla 7. Ventanas de mantenimiento a herramientas de ciberseguridad.

N°	HERRAMIENTA	FECHA DE ACTUALIZACIÓN
1	Firmware del equipo FortiSIEM	20/05/2024
2	FortiGate, FortiAnalizer, FortiWeb	21/05/2024

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Para llevar a cabo la actualización de los equipos se realiza un levantamiento de información previo, con el fin de conocer los bugs reportados por fabricante pero que no alteraran el funcionamiento normal de los equipos.

Contactar al encargado de seguridad de la información en el Grupo Tic para más información detallada de cada evento, resultados y procedimientos.

5.3 Plan de Auditorías de Seguridad de la Información

Se realizó una auditoría por OCI LINEAMIENTO 11 Y 13, se entregaron los insumos y se está a la espera de resultados para una posterior retroalimentación de los hallazgos encontrados.

Para el SGSI se requiere realizar auditorías de seguridad para evidenciar el seguimiento y gestión del sistema, para ello se debe tener en cuenta lo siguiente:

Objetivo de la auditoría: Revisar el funcionamiento y mantenimiento del Sistema de Gestión de Seguridad de la Información del MINENERGÍA.

Alcance de la auditoría: El alcance de la auditoría abarca a todo el MINENERGÍA y sus procesos, teniendo como base de revisión la norma ISO 27001:2013 y el Modelo de Seguridad y Privacidad de MINTIC.

Criterios de auditoría: Normatividad vigente que aplique a la fecha, así mismo las Políticas, Procedimientos, Instructivos, Planes, Mapas de Riesgos de Seguridad de la Información, Informe de Revisión por la Dirección y el Plan de Seguridad de la información.

5.4 Plan de mejoramiento continuo

El mejoramiento continuo de seguridad de la información está estrechamente ligado a la ejecución de auditorías, con base en la auditoría realizada para el periodo se deben ejecutar las siguientes actividades una vez se cuente con el informe de auditoría:

- Revisar la eficacia de las acciones correctivas tomadas.
- Realizar los cambios al SGSI de ser necesario.

A partir de los hallazgos efectuados en auditorias anteriores, se hacia la recomendación de tener en las buenas prácticas de desarrollo un apartado de aplicación de código seguro. Teniendo en cuenta esto se hace el debido procesos y análisis y se establece los numerales 8 y 9 como se menciona al inicio de este informe de la ***"Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información y Nuevas Aplicaciones del Ministerio De Minas Y Energía"***

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

6. PLAN DE SENSIBILIZACIÓN Y CAPACITACIÓN

Como resultado de la aplicación del Procedimiento de capacitación y sensibilización de personal, el plan de sensibilización y capacitación es uno de los mecanismos por medio del cual la entidad hace que sus usuarios tomen conciencia de la política de seguridad de la información, su contribución a la eficacia del sistema de gestión de la SI, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información; y las implicaciones de la no conformidad con los requisitos del sistema de gestión de la SI.

6.1 Sensibilización

La comunicación es uno de los procesos más relevantes y complejos que lleva a cabo el ser humano. Por ello, es importante tomar conciencia y asumir el control de lo que se comunica para ser eficientes y obtener el máximo de las personas y las situaciones.

Las entidades han entendido la oportunidad de recurrir a acciones de información y comunicación, como parte de las campañas de sensibilización, con el objetivo de facilitar la apropiación de conocimiento e incentivar el cambio en la cotidianidad en los actores de su interés (colaboradores, ciudadanía en general, aliados, entre otros).

Entendiendo la diversidad de públicos del Ministerio y la renovación del personal de planta y de colaboradores, se ha planteado incluir acciones en diferentes momentos y pantallas, procurando incrementar el alcance de los contenidos propuestos.

RESULTADOS:

PRIMER TRIMESTRE

Para el corte a marzo del año 2024 el Grupo de Tecnologías de Información y las Comunicaciones ha empleado principalmente como medios de difusión:

- Jornada de inducción y reinducción
- Correo institucional **@seguridaddelainformacion**
- Pantallas del Ministerio

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

De la siguiente manera:

• *JORNADA DE INDUCCIÓN Y REINDUCCIÓN*

Para el año 2024 la rotación del personal del ministerio alcanzó el ingreso de 199 nuevos usuarios en el directorio activo, cifra cercana al 20% de la base de los colaboradores.

Durante la Jornada de Inducción y reinducción se realizó un ejercicio personalizado en el cual mediante una charla dinámica se socializó con los colaboradores, recientemente nombrados, tanto las funciones asignadas al *Grupo de Tecnologías de Información y Comunicación*, como los sistemas de información y los recursos disponibles para comunicarse con los usuarios del Ministerio, dedicando un espacio a resaltar la importancia de leer y compartir los TIPTIC.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

1

2

3

4

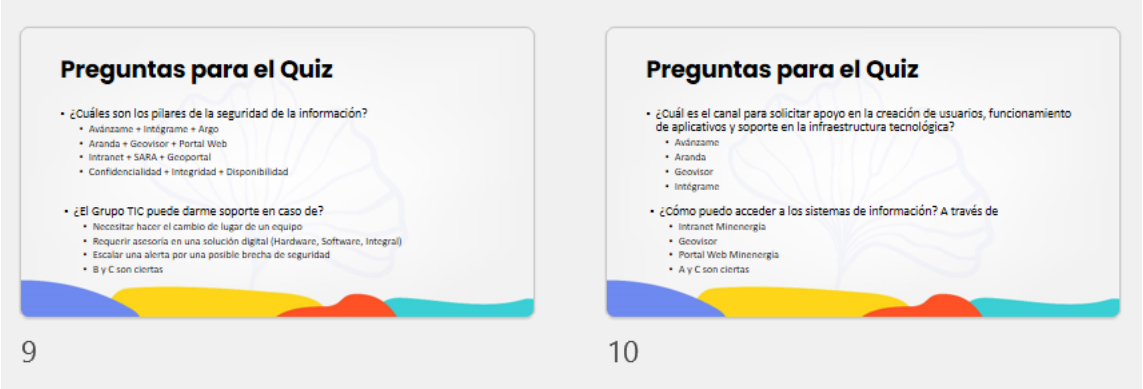
5

6

7

8

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300



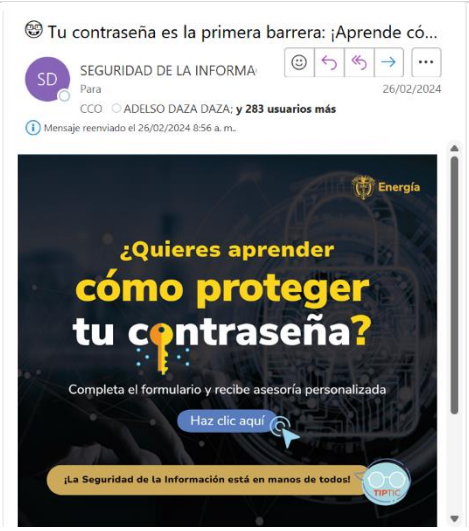
• *CORREO INSTITUCIONAL*

Este se emplea para el envío de piezas gráficas desde la cuenta de **@seguridaddelainformacion,**.

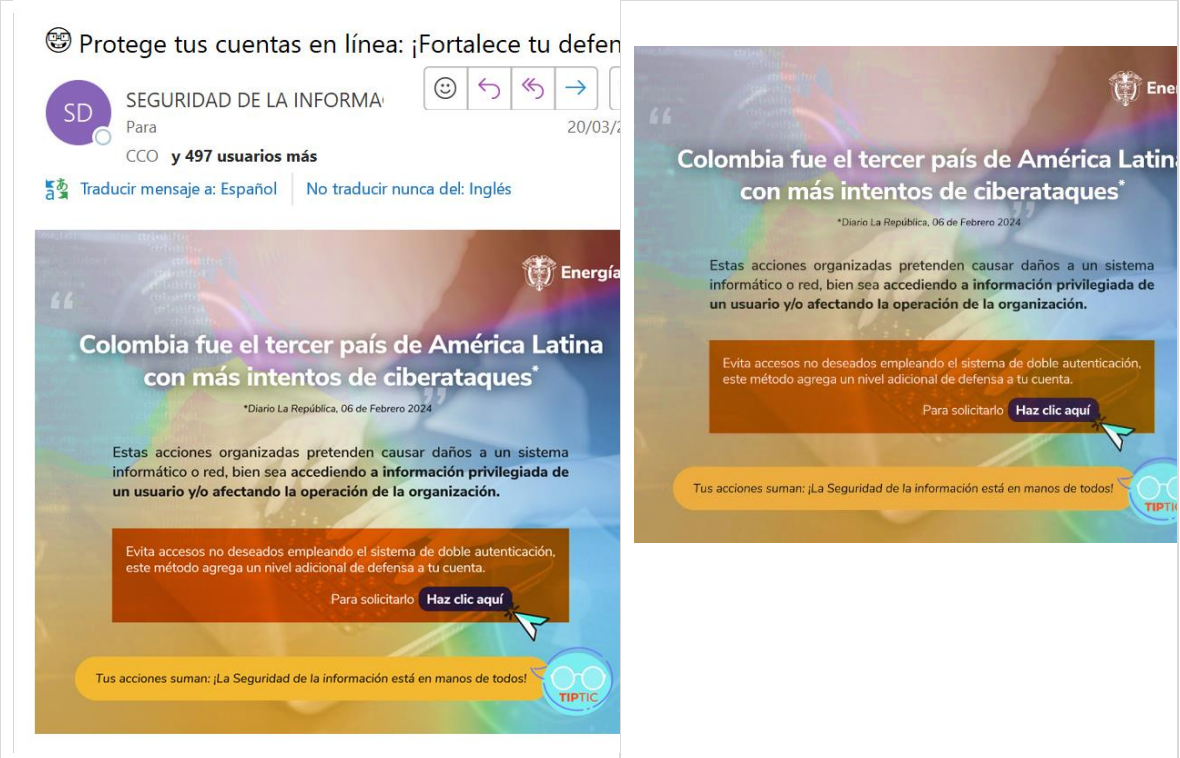
Correo Electrónico	Detalle de la referencia
	

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300



Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300



Al realizar una revisión comparativa del alcance obtenido, encontramos que los contenidos publicados va en ascenso siguiendo la tendencia de ingreso de colaboradores teniendo un alcance mínimo de 46% y llegando hasta máximo el 62%

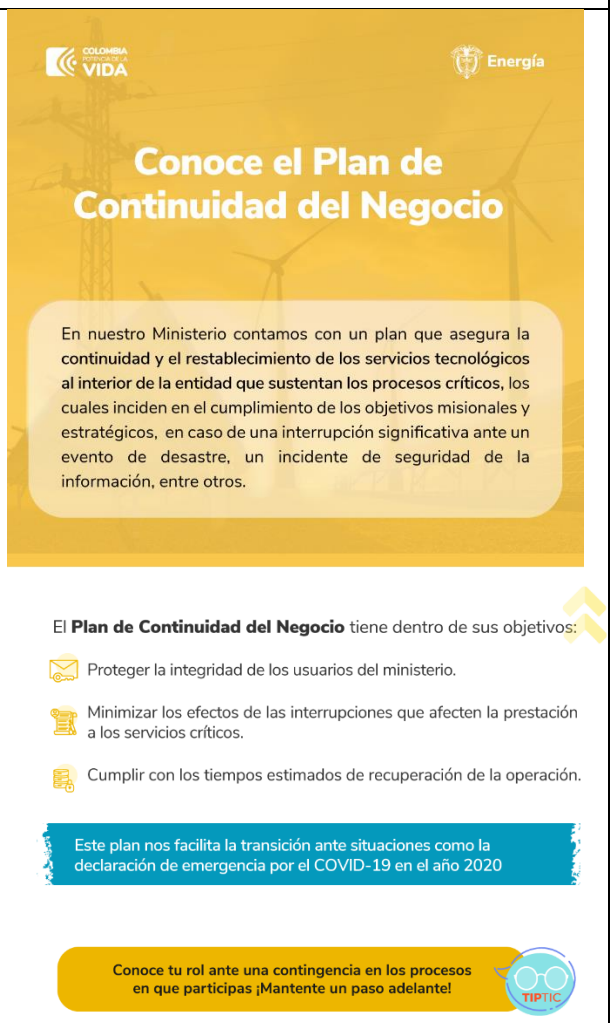
Continuaremos revisando constantemente los contenidos de este programa y su desempeño en lectura, con el fin de lograr la mejor adherencia de las buenas prácticas entre los usuarios y usarías de las herramientas TIC.

SEGUNDO TRIMESTRE

En cuanto a la distribución de contenidos del plan mediante el correo institucional se hace una variación con relación al cronograma inicial debido la implementación de planes actualizaciones en bases de datos, mantenimiento a la red de wi-fi entre otras ventanas requeridas para el periodo observado, por lo cual se planteó con el equipo de TICS el uso de un correo alterno para este tipo de alertas entre los usuarios Minenergía. En este proceso se probó el uso de la cuenta *notificacionestic*, el cual fue descartado por permisos.

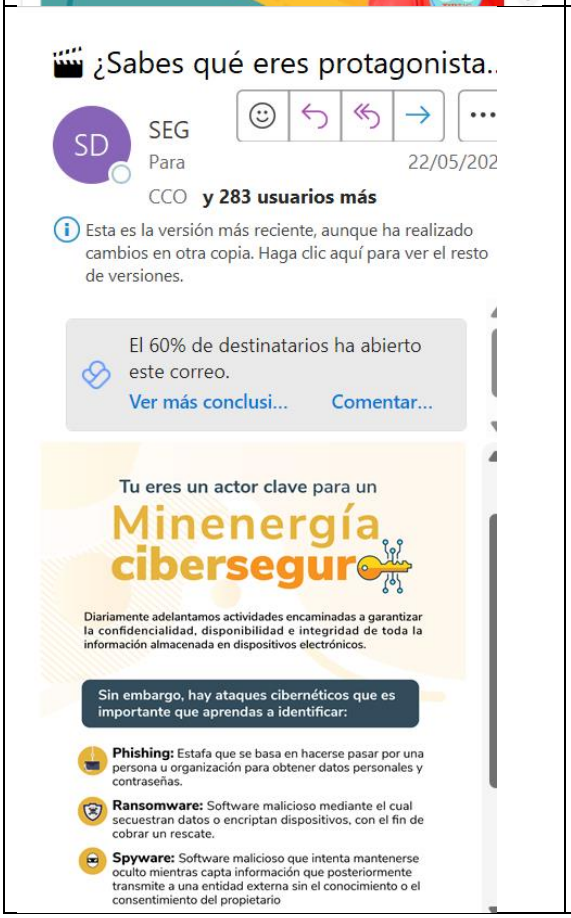
Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

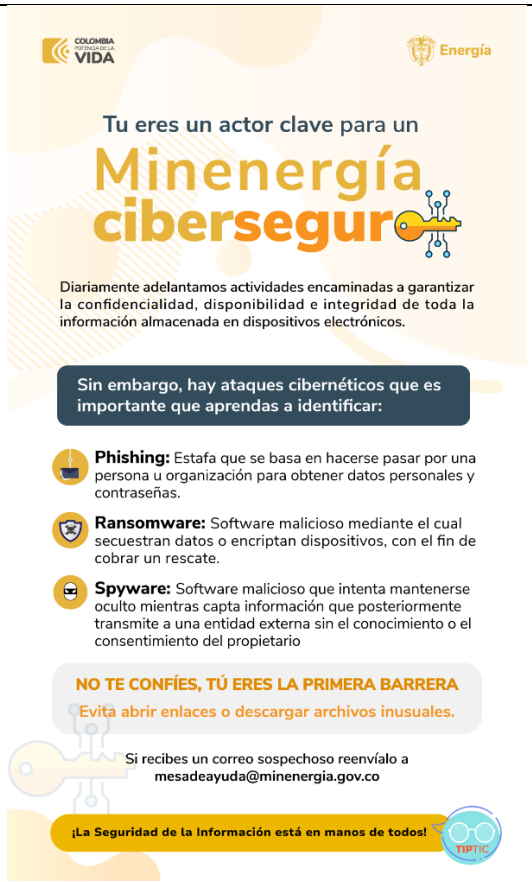
La apertura de los correos socializados oscila para este trimestre oscila entre el 58 y el 67% de apertura, manteniendo la tendencia que los funcionarios sean los usuarios que más frecuentemente abren los contenidos publicados frente los contratistas.

EVIDENCIA DE PUBLICACIÓN	PIEZA
	

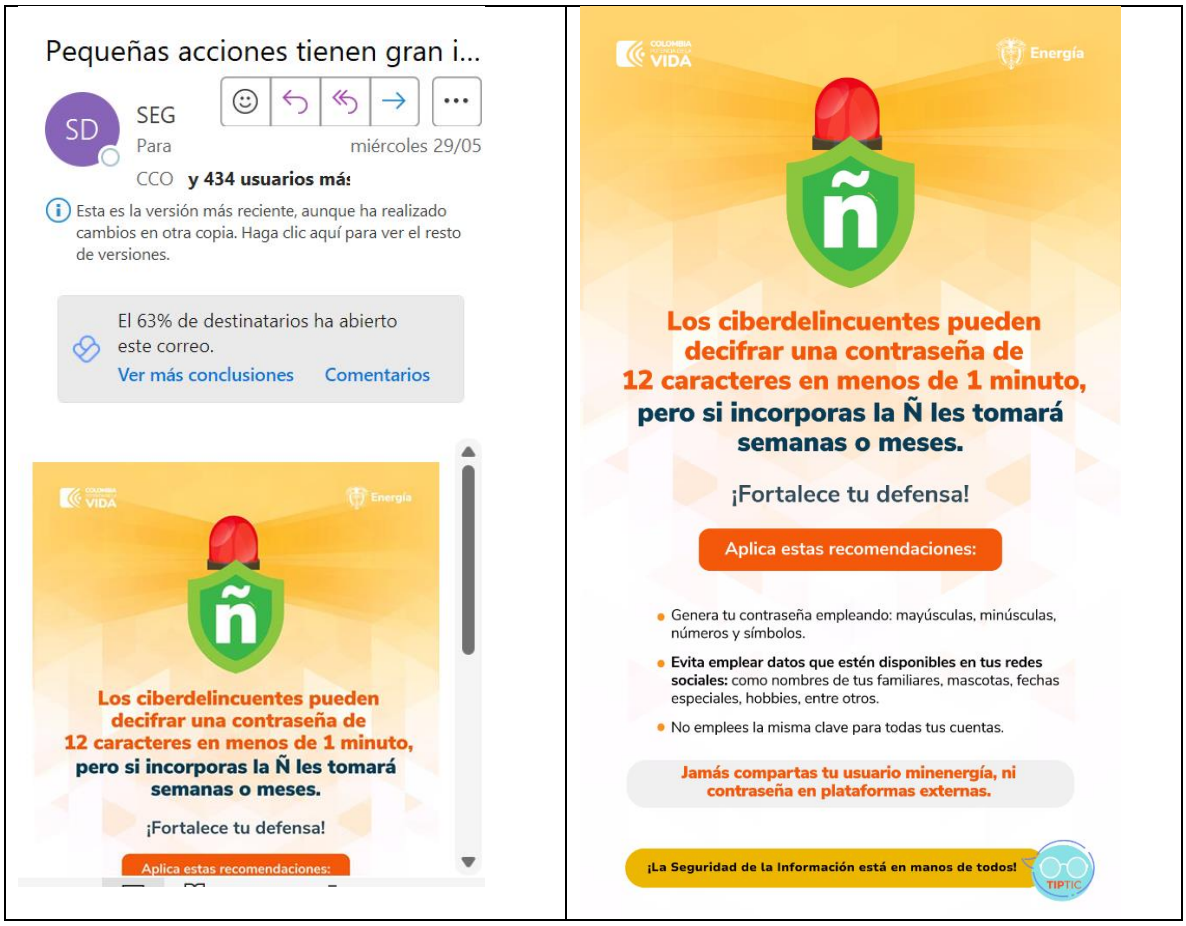
Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300





Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300



Continuaremos revisando constantemente los contenidos de este programa y su desempeño en lectura, para adherir las buenas prácticas entre los usuarios y usar las herramientas TIC.

6.2 Capacitación

Se viene trabajando en la actualización de contenidos de dos capacitaciones, la primera en generalidades de la seguridad de la información.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Con la finalidad de enriquecer los procesos se participa en la jornada de capacitación del Comando Conjunto de Ciberseguridad y Ciberdefensa, encontrando información relevante que se incorpora al proceso:

Para el segundo trimestre se hace un análisis de requerimientos según las necesidades identificadas en las dependencias, de esta manera se establece una hoja de ruta para las futuras capacitaciones previstas a desarrollarse en el tercer y cuarto trimestre del año 2024, con el objetivo de crear una capacidad distintiva en todos los funcionarios del Minenergia.

Ministerio de Minas y Energía
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

Energía