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

Título:

Seguimiento Plan de Seguridad y Privacidad de la Información –

Tercer Trimestre 2024

Elaboró:

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

Leidy Paola Galindo Acevedo

Oscar Sanchez Sanchez

Andrés Camilo Molano Mendieta

Entidad:

Ministerio de Minas y Energía

Bogotá, 31 de octubre 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

1. PROCESO 3

2. RESPONSABLE DEL PROCESO 3

3. DESCRIPCIÓN INFORME 3

4.1 Gestión de Activos de Información 4

4.2 Gestión de Riesgos de Seguridad de la Información 6

4.2 Riesgos de Seguridad y Privacidad de la Información 25

4.3 Tratamiento de Riesgos 48

4.4 Gestión de políticas y procedimientos 49

4.5 Gestión de recursos de seguridad 51

5. PLAN DE SEGUIMIENTO Y EVALUACIÓN DE LA IMPLEMENTACIÓN Y MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN 55

5.1 Gestión de indicadores 55

5.2 Gestión de Vulnerabilidades 56

5.3 Plan de Auditorías de Seguridad de la Información 67

5.4 Plan de mejoramiento continuo 67

PLAN DE SENSIBILIZACIÒN Y CAPACITACIÒN 68

6.1 Sensibilización 69

6.1 Capacitación 81

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 delestado 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. Para el primer trimestre del año en curso, se ha adelantado 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. Para el segundo trimestre se hace la inclusión de información de la nueva categorización implementada en el nuevo mapa de procesos, actualización de TRD con el fin de pasar a revisión directiva y proceder a la recolección y divulgación que permita a las dependencias nutrir dicho proceso.

En este mismo sentido, se actualiza el material de apoyo a la capacitación para orientar a los usuarios en el ejercicio y 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.

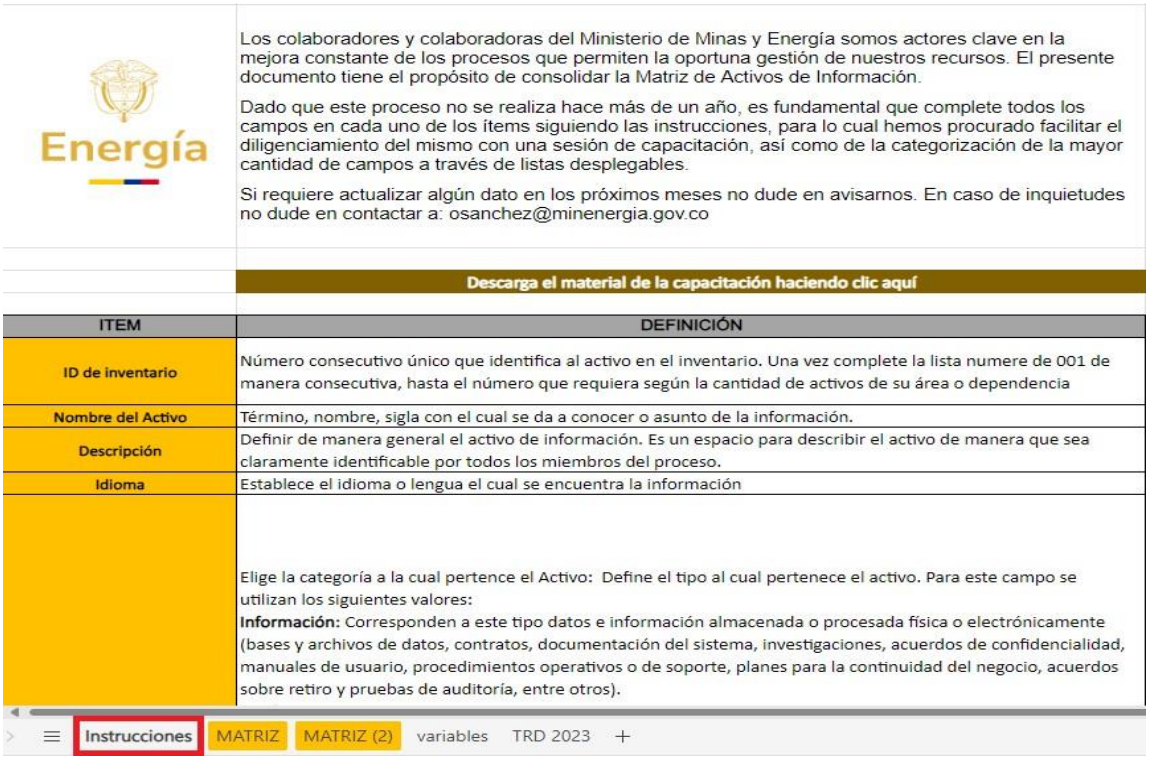
En el tercer semestre, se implementó un plan piloto que integró un manual de instrucciones diseñado para clarificar el procedimiento de diligenciamiento de la matriz de activos. Se realizaron ajustes en la evaluación de la criticidad de los activos de información, considerando las últimas actualizaciones de las normas ISO/IEC 27001 e ISO/IEC 27005. Además, se destacó claramente la normativa aplicable, que especificaba el custodio responsable de cada activo. Este plan piloto se aplicó inicialmente en el grupo de Tecnologías de la Información y las Comunicaciones (TICS) (logrando 20 activos de información). La retroalimentación obtenida indicó que la matriz, junto con los procedimientos e instrucciones, resultó ser intuitiva y exhaustiva. Se incluyó un apartado de observaciones para cada activo, lo que permitió una evaluación más holística e integral de su uso, custodia e importancia, más allá de su simple criticidad.

Con base en lo anterior, se establece un cronograma para el cuarto trimestre de 2024, que contempla una fase inicial de divulgación. En esta etapa, se explicará la importancia de gestionar adecuadamente los activos de información, así como su uso y direccionamiento. Posteriormente, se llevará a cabo la fase de gestión, en la que cada dependencia del Ministerio de Minas y Energía diligenciará la matriz con los detalles pertinentes. Este proceso estará

Ministerio de Minas y Energía

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

supervisado por el responsable de seguridad de la información del grupo de Tecnologías de la Información y las Comunicaciones (TIC). Finalmente, la fase de cierre consistirá en evaluar el proceso y los resultados, con el objetivo de implementar mejoras continuas. Esto permitirá obtener una base de activos que servirá como insumo para la estructuración de otros procesos relacionados con la ciberseguridad y la ciberdefensa. (Para más información del documento-matriz de gestión de activos de información final, remitirse al responsable de seguridad de la información a cargo).



Los colaboradores y colaboradoras del Ministerio de Minas y Energía somos actores clave en la mejora constante de los procesos que permiten la oportuna gestión de nuestros recursos. El presente documento tiene el propósito de consolidar la Matriz de Activos de Información.

Dado que este proceso no se realiza hace más de un año, es fundamental que complete todos los campos en cada uno de los ítems siguiendo las instrucciones, para lo cual hemos procurado facilitar el diligenciamiento del mismo con una sesión de capacitación, así como de la categorización de la mayor cantidad de campos a través de listas desplegables.

Si requiere actualizar algún dato en los próximos meses no dude en avisarnos. En caso de inquietudes no dude en contactar a: osanchez@minenergia.gov.co

Descarga el material de la capacitación haciendo clic aquí

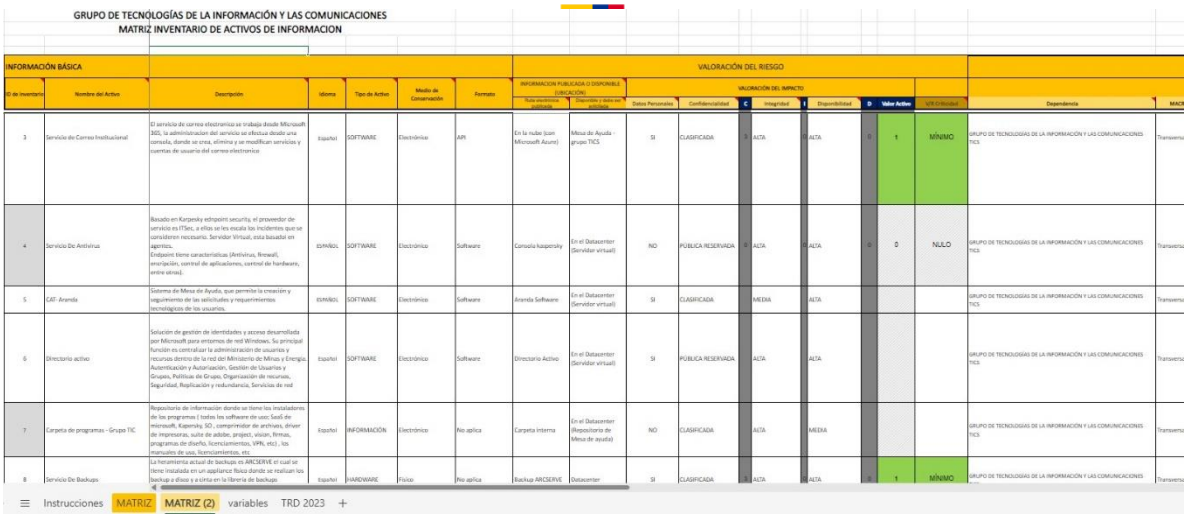
ITEM	DEFINICIÓN
ID de inventario	Número consecutivo único que identifica al activo en el inventario. Una vez complete la lista numere de 001 de manera consecutiva, hasta el número que requiera según la cantidad de activos de su área o dependencia
Nombre del Activo	Término, nombre, sigla con el cual se da a conocer o asunto de la información.
Descripción	Definir de manera general el activo de información. Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.
Idioma	Establece el idioma o lengua el cual se encuentra la información
	Elige la categoría a la cual pertence el Activo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores: **Información:** Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente (bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros).

Instrucciones | MATRIZ | MATRIZ (2) | variables | TRD 2023 | +

Imagen [1]. Vista inicial de instructivo e información para el diligenciamiento de la matriz de activos de información 2024.

Ministerio de Minas y Energía

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



GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
MATRIZ INVENTARIO DE ACTIVOS DE INFORMACION

INFORMACIÓN BÁSICA							VALORACIÓN DEL RIESGO									
							INFORMACION PUBLICADA O DISPONIBLE (USUARIOS)		VALORACIÓN DEL IMPACTO							
ID de inventario	Nombre del Activo	Descripción	Idioma	Tipo de Activo	Medio de Conservación	Formato	Nota electrónica publicada	Disponible y dada en archivos	Datos Personales	Confidencialidad	C	Integridad	I	Disponibilidad	D	Valor Activo	VR Criticidad	Dependencia	MAC
3	Servicio de Correo Institucional	El servicio de correo electrónico se trabaja desde Microsoft 365, la administracion del servicio se efectua desde una consola, donde se crea, elimina y se modifican servicios y cuentas de usuario del correo electronico	Español	SOFTWARE	Electrónico	API	En la nube (con Microsoft Azure)	Mesa de Ayuda - grupo TICS	SI	CLASIFICADA	3	ALTA	3	ALTA	3	1	MÍNIMO	GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TICS	Transversa
4	Servicio De Antivirus	Basado en Karpesky edrpoint security, el proveedor de servicio es ITSec, a ellos se les escala los incidentes que se consideren necesario. Servidor Virtual, esta basado en agentes. Endpoint tiene caracteristicas (Antivirus, firewall, encripción, control de aplicaciones, control de hardware, entre otras).	ESPAÑOL	SOFTWARE	Electrónico	Software	Consola kaspersky	En el Datacenter (Servidor virtual)	NO	PUBLICA RESERVADA	0	ALTA	3	ALTA	3	0	NULO	GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TICS	Transversa
5	CAT- Aranda	Sistema de Mesa de Ayuda, que permite la creación y seguimiento de las solicitudes y requerimientos tecnológicos de los usuarios.	ESPAÑOL	SOFTWARE	Electrónico	Software	Aranda Software	En el Datacenter (Servidor virtual)	SI	CLASIFICADA	2	MEDIA	2	ALTA				GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TICS	Transversa
6	Directorio activo	Solución de gestión de identidades y acceso desarrollada por Microsoft para entornos de red Windows. Su principal función es centralizar la administración de usuarios y recursos dentro de la red del Ministerio de Minas y Energía. Autenticación y Autorización, Gestión de Usuarios y Grupos, Políticas de Grupo, Organización de recursos, Seguridad, Replicación y redundancia, Servicios de red	Español	SOFTWARE	Electrónico	Software	Directorio Activo	En el Datacenter (Servidor virtual)	SI	PUBLICA RESERVADA	3	ALTA	3	ALTA				GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TICS	Transversa
7	Carpeta de programas - Grupo TIC	Repositorio de información donde se tiene los instaladores de los programas (todos los software de uso: Sosfi de microsoft, Kapersky, SO , comprimidor de archivos, driver de impresoras, suite de adobe, project, vision, firmas, programas de diseño, licenciamientos, VPN, etc) , los manuales de uso, licenciamientos, etc	Español	INFORMACIÓN	Electrónico	No aplica	Carpeta interna	En el Datacenter (Repositorio de Mesa de ayuda)	NO	CLASIFICADA	2	ALTA	2	MEDIA				GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TICS	Transversa
8	Servicio De Backups	La herramienta actual de backups es ARCSERVE el cual se tiene instalada en un appliance físico donde se realizan los backup a disco y a cinta en la libreria de backups	Español	HARDWARE	Físico	No aplica	Backup ARCSERVE	Datacenter	SI	CLASIFICADA	3	ALTA	3	ALTA	3	1	MÍNIMO	GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES TICS	Transversa

Instrucciones | MATRIZ | MATRIZ (2) | variables | TRD 2023 | +

Imagen [2]. Proceso de ejemplo de diligenciamiento de la matriz de activos de información.

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:

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:

Ministerio de Minas y Energía

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

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 como resultados:

Mes	Resultado
Abril	-De acuerdo con el diagnostico 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 diagnostico 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.
Junio	-De acuerdo con el diagnostico 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.

Ministerio de Minas y Energía

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

Para el tercer trimestre se hace el proceso nuevamente cumpliendo con el cronograma y frecuencia pertinentes obteniendo los siguientes resultados:

Mes	Resultado
Julio	-De acuerdo con el diagnostico 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.
Agosto	-De acuerdo con el diagnostico de los diez (11) 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.
Septiembre	De acuerdo con el diagnostico 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.

Ministerio de Minas y Energía

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

- 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:

  El mantenimiento preventivo de equipos es crucial 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.

  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 intervino **207 equipos en el mes de junio 2024.**

  Los procesos y hallazgos encontrados durante este mantenimiento se encuentran en el informe de mantenimiento preventivo junio 2024 B2B, si se requiere más información gestionarla con el responsable de mantenimiento preventivo de la mesa de ayuda .

  Para el tercer trimestre 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 yen la sede del Archivo en la Carrera 50 N°26 – 20, Bogotá., se intervino **95 equipos en el trimestre Julio - septiembre 2024.**

  Los procesos y hallazgos encontrados durante este mantenimiento se encuentran en el informe de mantenimiento preventivo septiembre 2024 B2B, si se requiere más

Ministerio de Minas y Energía

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

información gestionarla con el responsable de mantenimiento preventivo de la mesa de ayuda .

- 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 para el segundo trimestre:

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.

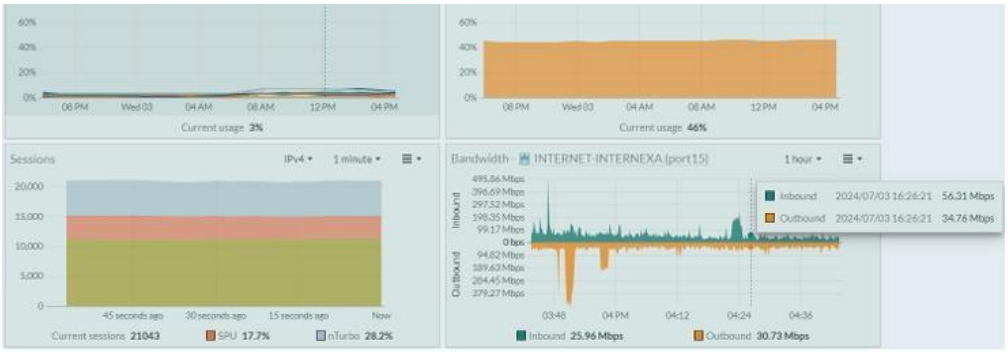


Imagen [3] . Ejemplo de trafico de consumo de red y de recursos por FW, segundo trimestre.

Ministerio de Minas y Energía

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

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:

Entitlement	Status	
Advanced Malware Protection	Licensed (Expiration Date: 2026/12/29)	
Attack Surface Security Rating	Not Licensed	Purchase
Data Loss Prevention (DLP)	Not Licensed	
Email Filtering	Licensed (Expiration Date: 2026/12/29)	
Intrusion Prevention	Licensed (Expiration Date: 2026/12/29)	
Operational Technology (OT) Security Service	Not Licensed	Purchase
Web Filtering	Licensed (Expiration Date: 2026/12/29)	

Imagen [4]. 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

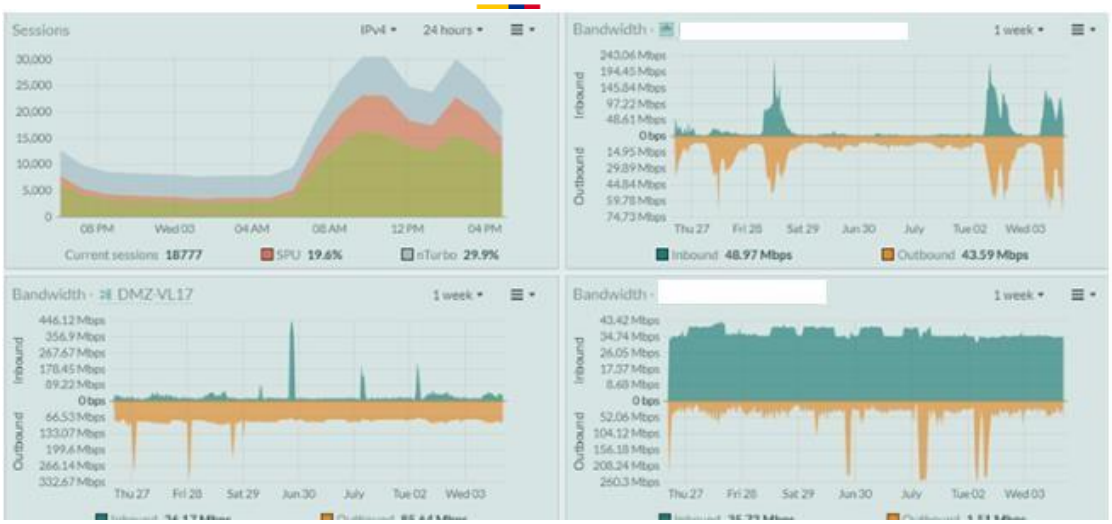


Imagen [5]. Gráfico de consumo de datos del FW , pruebas tomadas en ciclo de vida activo, segundo trimestre.

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 puedansurgir a nivel web
Además, 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 MME

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.

k. Conexiones de VPN FortiClient:

Ministerio de Minas y Energía

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

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 MME 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 [6]. 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.

I. 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:

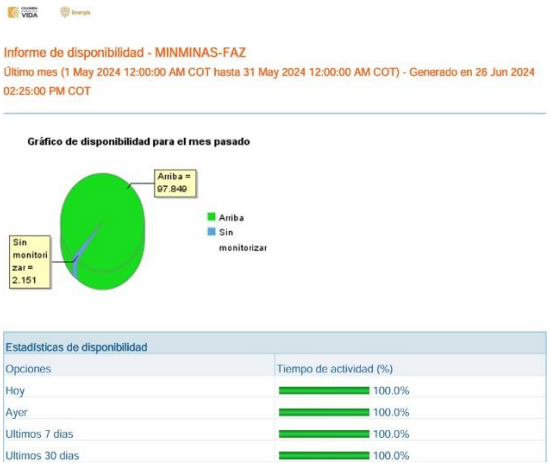


Imagen [7]. Ejemplo de visualización grafica de disponibilidad de recursos

Ministerio de Minas y Energía

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

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.

m. 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 MME.

Destacando los siguientes ítems:

i. Claves de licencia
ii. Distribución de la protección
iii. Bases de datos de antivirus.
iv. Estado de protección.
v. Informe de amenazas vigentes.
vi. Dispositivos más afectados.
vii. Informe de despliegue.
viii. Informe de vulnerabilidades identificadas.
ix. Control web.
x. 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

Ministerio de Minas y Energía

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

- 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

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.

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. El informe 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. Se 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 MME 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

Ministerio de Minas y Energía

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

(velocidad, picos de consumo y/o eventos relacionados) remitirse al 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 para el tercer trimestre :

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 menor al 45 % y CPU menor a 18%**; en datos registrados en la consola web que visualizan gráficamente su conducta, debido a que el FortiGate es una plataforma dinámica que ejecuta múltiples procesos y solicitudes en tiempo real, en ocasiones puede ser bastante pesados y por sí mismos pueden ser consumidores de recursos. En este caso se puede observar que los recursos de la maquina se encuentra en nivel normal, sin embargo, si se evidencia un incremento respecto al trimestre anterior, se puede deber a los diferentes usuarios nuevos que han ingresado.

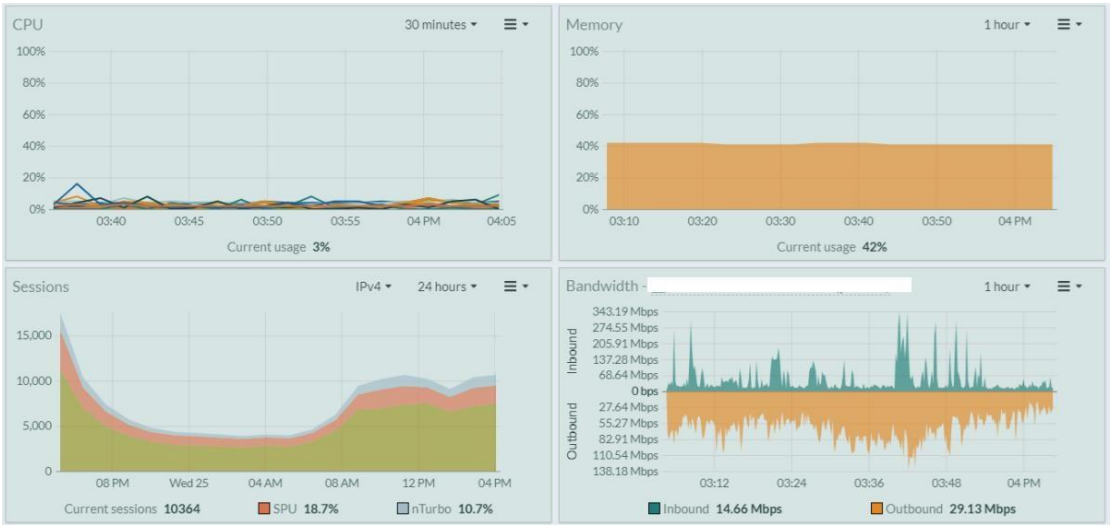


Imagen [8] . Ejemplo de trafico de consumo de red y de recursos por FW, tercer trimestre.

Importante destacar que para el tercer trimestre se realizó un apagado controlado por mantenimiento eléctrico del ministerio de manera que el estatus de “uptime” es de pocos días, sin embargo, este no ha parado su operación por fallas técnicas.

Ministerio de Minas y Energía

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

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:

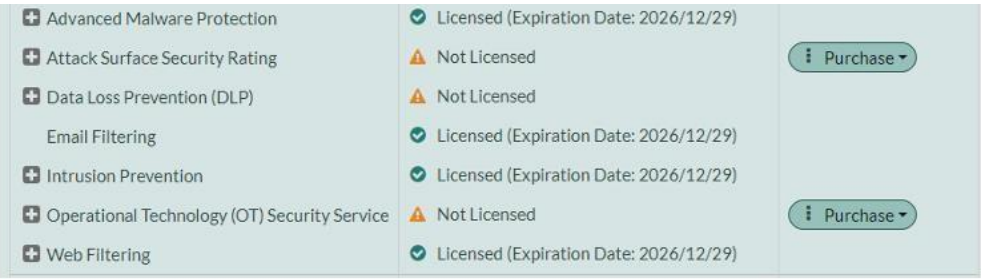


Imagen [9]. Estatus de licenciamiento de las herramientas de monitoreo y defensa

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, para este tercer trimestre se hacen cambios en la función de Override que queda en modo disable , esto quiere decir que si se presenta una falla en el master entra en funcionamiento el esclavo y cuando reanude operación se debe hacer un cambio manual para quedar nuevamente en la jerarquía adecuada. Ademas se realiza un proceso de verificación con comando desde el master para identificar la correcta sincronización de los equipos, dando respuesta y resultados acordes.

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.

Ministerio de Minas y Energía

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

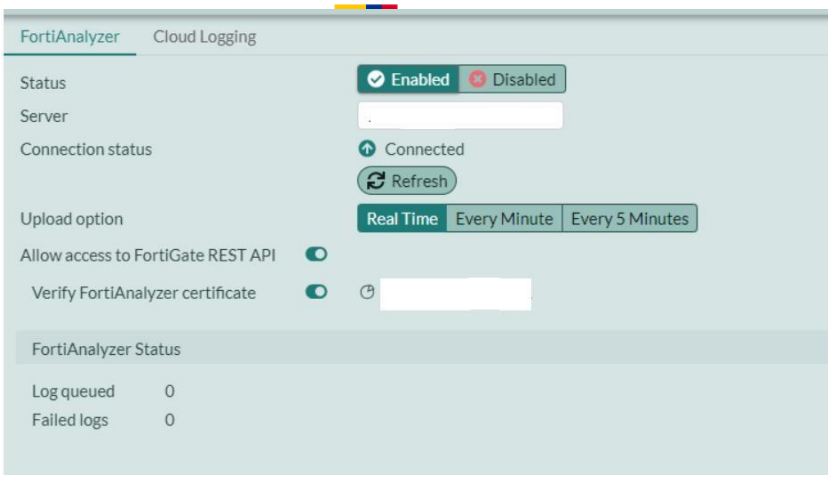


Imagen [10]. Estatus de FortiAnalyzer, conectado y dirigido a un servidor puntual.

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.

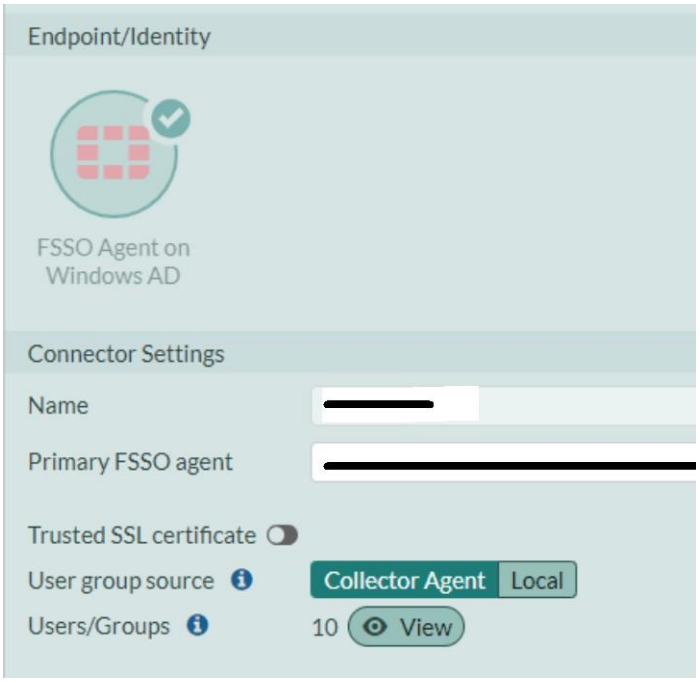


Imagen [11]. Configuración Agente FSSO, conectado y dirigido a un servidor puntual.

Ministerio de Minas y Energía

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

d. **Consumo de canal de datos:** Se realiza la revisión del consumo del canal evidenciando que si se encuentra saturado, pero solo el enlace a la MPLS que se tiene hacia el datacenter alterno esto se debe a que se están replicando algunos servidores para posteriormente realizar pruebas de DRP.

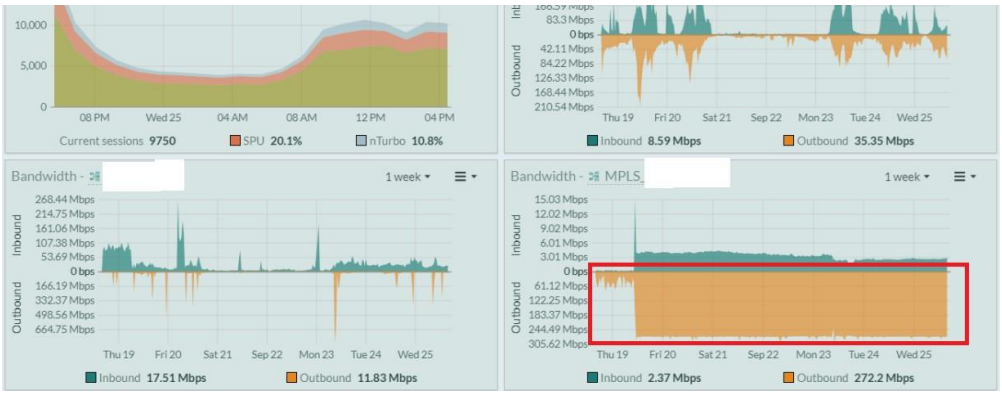


Imagen [12] .Gráfico de consumo de datos del FW , pruebas tomadas en ciclo de vida activo, tercer trimestre.

e. **Afinamiento de políticas en el WAF:** Se depuran las aplicaciones que deben estar publicadas en internet quitando algunas que ya no se usan como tablerospbi, archergrc, compartomienergia, reportesintegracion. 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

f. **Revisión de políticas hacia zona DMZ:** Se configuran políticas limitando accesoy 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 Ministerio de Minas y Energia, generando una base datos correspondiente al **"BlackList"** .

h. 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

k. Se actualizan firmware de equipos Firewall y Fortianalizer.

l. Conexiones de VPN FortiClient :

Se llevó a cabo un análisis detallado de los usuarios con acceso a la VPN del Ministerio de Minas y Energía, en el que se determinó que una gran cantidad de ellos no requiere este acceso para cumplir con sus funciones. Dado que no tienen la responsabilidad de gestionar, manipularo agregar información en los sistemas internos del ministerio, el acceso a la VPN no es esencial ni justificado para su actividad diaria.

A partir de este análisis, se decidió optimizar los permisos y establecer un nuevo grupo de usuarios dentro del firewall (FW), donde se asignaron exclusivamente aquellas cuentas que realmente necesitan acceso a los sistemas internos de información. Este nuevo grupo permite una mejor segmentación y control de usuarios, garantizando que solo quienes tengan responsabilidades directas sobre la información crítica del ministerio accedan a la VPN, reduciendo así posibles riesgos de seguridad y optimizando el uso de los recursos tecnológicos.

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

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

Para el tercer trimestre del año, y reconociendo la importancia crítica de la disponibilidad de los sistemas de seguridad Firewall (FW), Web Application Firewall (WAF) y FortiAnalyzer (FAZ), se ha realizado un análisis detallado de su rendimiento. Este análisis ha permitido establecer las siguientes estadísticas clave que reflejan su funcionamiento y eficiencia operativa durante este período.

Ministerio de Minas y Energía

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

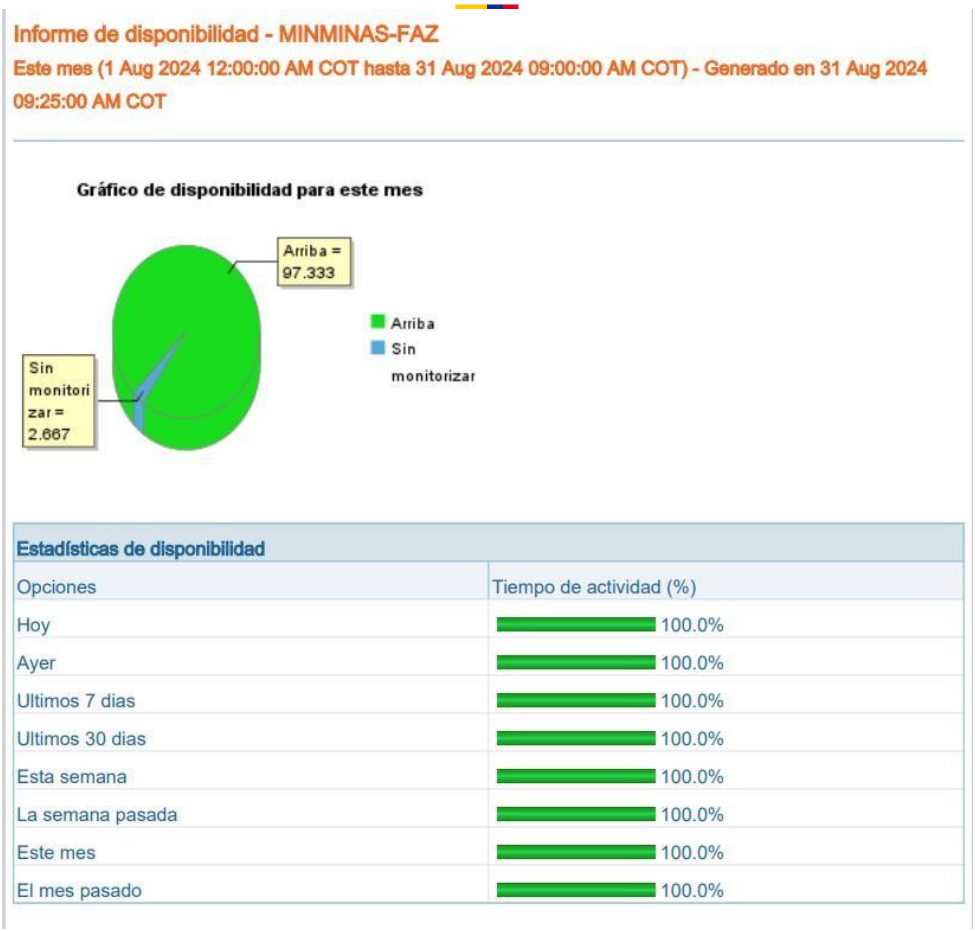


Imagen [13]. Ejemplo de visualización grafica de disponibilidad de recursos, WAF mes de agosto

Dicha estructura establece tiempos de disponibilidad por intervalos predefinidos (frecuencia de escaneo) por cada una de las herramientas, los resultados identificados para el tercer trimestre del año 2024 es que existe una disponibilidad 24/7 (cumplimiento del 97.3%) con una franja de monitorización (no necesariamente indisponibilidad) del 2.7%, para mayor detalle puede consultar al responsable de seguridad de la información a cargo, ya que la razón de este monitoreo no puede ser expuesta de manera pública.

Ministerio de Minas y Energía

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

n. **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 MME.

Destacando los siguientes ítems:

xi. Claves de licencia
xii. Distribución de la protección
xiii. Bases de datos de antivirus.
xiv. Estado de protección.
xv. Informe de amenazas vigentes.
xvi. Dispositivos más afectados.
xvii. Informe de despliegue.
xviii. Informe de vulnerabilidades identificadas.
xix. Control web.
xx. Estado de los servidores

Dentro de los hallazgos determinados por este informe para el tercer trimestre se tiene lo siguiente:

7. **Licenciamiento:** En el mes de julio se tienen 1200 licencias adquiridas, 607 en uso y 593 disponibles, para el mes de agosto se tienen 1200 licencias adquiridas, 631 en uso y 569 disponibles

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

9. **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: # 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

Ministerio de Minas y Energía

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

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

10. Informe de amenazas:

En el mes de julio, se identificaron XX detecciones de enlaces maliciosos, los cuales fueron rápidamente identificados y eliminados, evitando así cualquier posible impacto en los sistemas de información del Ministerio de Minas y Energía.

Para el mes de agosto, el número de detecciones aumentó a XXXX, las cuales fueron bloqueadas, y la mayoría de ellas se catalogaron como virus informáticos provenientes de intentos de intrusión en los sistemas del Ministerio. De las amenazas detectadas, XXX fueron eliminadas de manera efectiva, pero se descubrieron dos agentes maliciosos tipo troyano. Estos troyanos se propagaban a través de correos electrónicos, sitios web maliciosos y descargas de archivos no seguros.

Los troyanos identificados fueron aislados y analizados en un entorno controlado de SandBox, donde se determinó que tenían la capacidad de deteriorar el rendimiento del sistema y descargar malware adicional de manera remota. Este hallazgo subraya la importancia de mantener un monitoreo continuo y proactivo, además de reforzar las medidas de ciberseguridad para prevenir la entrada y propagación de este tipo de amenazas en la red del Ministerio.

Para más información y detalle sobre el informe remitirse al responsable de seguridad de la información a cargo.

11. Dispositivos infectados:

Se ha identificado la presencia de posibles dispositivos infectados, por lo que es necesario proceder con el protocolo de limpieza y extracción del malware de forma inmediata. Dada la naturaleza crítica de esta situación, se subraya la importancia de llevar a cabo este proceso de manera minuciosa, asegurando que todos los sistemas afectados sean completamente restaurados a un estado seguro.

Ministerio de Minas y Energía

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

Como parte de las acciones prioritarias, se ha determinado la necesidad de fortalecer las políticas, sistemas y lineamientos de seguridad y privacidad de la información. Esto se debe a un notable incremento exponencial en los intentos de intrusión registrados entre los meses de julio y agosto, lo que representa un riesgo significativo para la infraestructura tecnológica del Ministerio. Este aumento podría estar relacionado tanto con ataques dirigidos como con errores humanos derivados de malas prácticas de seguridad digital, lo que resalta la importancia de mejorar la formación y concientización del personal en ciberseguridad.

Es crucial implementar medidas correctivas inmediatas para mitigar estos riesgos y prevenir futuros incidentes. Para obtener más detalles sobre el proceso a seguir y los próximos pasos a tomar, se recomienda contactar al responsable de seguridad de la información, quien está a cargo de coordinar las acciones necesarias y garantizar el cumplimiento de los protocolos de seguridad establecidos.

12. Validación del estado de los servidores:

Durante el tercer trimestre, se han detectado novedades significativas en el análisis de los servidores del Ministerio de Minas y Energía. Estas observaciones subrayan la importancia de ejecutar de manera rigurosa los procesos de seguridad de la información para prevenir vulnerabilidades futuras. Aunque se ha evidenciado un avance en el plan de mejora establecido, aún es esencial continuar con las acciones correctivas y preventivas que permitan asegurar la integridad de los sistemas.

El grupo TIC del Ministerio ha estado a cargo de las subsanaciones identificadas en los informes previos, particularmente en lo relacionado con los servidores y la depuración de usuarios en el directorio activo que se gestiona internamente. Estas tareas son clave para garantizar que solo usuarios autorizados tengan acceso a los recursos internos, reduciendo así el riesgo de accesos no autorizados y posibles incidentes de seguridad.

Para obtener un análisis más detallado y seguimiento de estas actividades, es necesario contactar al responsable de seguridad de la información a cargo, quien podrá proporcionar información actualizada sobre el estado del plan de mejora, las acciones pendientes y las estrategias futuras para mitigar riesgos potenciales en la infraestructura tecnológica del Ministerio.

Ministerio de Minas y Energía

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

- **Informes de operación y disponibilidad de canales con los diferentes operadores de telecomunicaciones de los meses de julio, agosto y septiembre:**

  El Informe de gestión mensual contiene datos clave que permiten evaluar el nivel de cumplimiento del acuerdo firmado entre el Ministerio de Minas y Energía (MME) y el operador. Este informe abarca los resultados y el análisis de la gestión de los servicios correspondientes al tercer trimestre de 2024, presentando una discriminación detallada por cada uno de los meses del período.

  El documento incluye el nivel de cumplimiento de los servicios contratados, destacando que los Acuerdos de Nivel de Servicio (SLA) evaluados muestran un desempeño óptimo, con un cumplimiento del 100% de la operación. No se registraron eventos ni interrupciones significativas durante los meses analizados, lo que indica una operación fluida y acorde con los términos establecidos en el contrato.

  Para obtener más información sobre aspectos técnicos específicos, como velocidad de la conexión, picos de consumo y cualquier otro evento relacionado con la operación, se recomienda dirigirse al responsable de seguridad de la información a cargo. Esta persona podrá proporcionar detalles adicionales sobre los parámetros técnicos y el rendimiento del servicio durante el periodo en cuestión.

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 Ministerio de Minas y Energia, puede remitirse al siguiente con el responsable de seguridad de la información a cargo.

4.2 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

  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:

Ministerio de Minas y Energía

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

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 checklist de código seguro.

No	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.

Para el tercer trimestre se anexa el uso de los diferentes de lenguajes de programación que maneja el equipo de desarrollo y sobre que sistemas de información (remitirse al equipo de desarrollo para saber dichos activos de información)y software se encuentran actualmente, además se determinan las preguntas objeto de "checklist" para poder determinar la hoja de ruta del desarrollo.

Ministerio de Minas y Energía

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

- **Python:** Es un lenguaje de alto nivel de programación y es muy pragmático en la legibilidad de su código, se utiliza para desarrollar aplicaciones de todo tipo, web, local, hibrido, entre otros.

- **Java:** Permite escribir, compilar, depurar diferentes funcionalidades orientado a objetos de los sistemas de información.

- **Java Script:** Es un lenguaje de programación que es similar a Java teniendo en cuenta que estos mismos están orientado a objetos lo que permite que tenga un mayor manejo en la interpretación y el dialecto en los prototipos.

- **CSS:** Es un lenguaje que abarca toda la estructura de diseño visual y/o gráfico y se enfoca en desarrollo web.

- **HTML 5:** Permite crear la estructura de páginas web, donde se incorporan posteriormente imágenes, textos, vídeos y todo tipo de material multimedia de forma que se pueda visualizar correctamente.

- **SQL:** El lenguaje de consulta estructurada (SQL) es un lenguaje de consulta popular que se usa con frecuencia en todos los tipos de aplicaciones. Analistas y desarrolladores de datos aprenden y usan SQL porque se integra bien con los diferentes lenguajes de programación.

- **Flutter:** Permite crear aplicaciones móviles nativas con una sola base de código, lo que significa que se puede usar un lenguaje de programación en la web

- **.NET:** Es una plataforma de código abierto que permite crear aplicaciones locales, web y móviles que se pueden ejecutar de forma nativa en cualquier sistema operativo. Este mismo incluye herramientas, bibliotecas y lenguajes que admiten el desarrollo de software moderno, escalable y de alto rendimiento.

Ministerio de Minas y Energía

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

Checklist de Seguridad en el Desarrollo de Software	
Patrones de Diseño Seguros	
Patrón de Diseño MVC (Model-View-Controller)	
☐	¿Existe una clara separación entre la lógica de negocio, la lógica de presentación y el control de flujo?
☐	¿Se han implementado medidas de seguridad en cada capa del patrón MVC?
Patrón de Diseño Singleton	
☐	¿Se utiliza el patrón Singleton para la gestión centralizada de configuración y recursos críticos?
☐	¿Se aseguran controles de acceso en la instancia Singleton?
Patrón de Diseño Decorator	
☐	¿Se aplican decoradores para añadir validación y autorización de manera consistente?
☐	¿Se utilizan decoradores para reforzar las verificaciones de seguridad?
Patrón de Diseño Factory	
☐	¿Se utiliza el patrón Factory para la creación de objetos complejos?
☐	¿Se incluyen controles de seguridad durante la creación de instancias?
Antipatrones a Evitar	
Antipatrón de Spaghetti Code	
☐	¿El código está organizado y es mantenible?
☐	¿Se evita la creación de código altamente acoplado y desorganizado?
Antipatrón de God Object	
☐	¿Se distribuyen las responsabilidades de manera adecuada entre los objetos?
☐	¿Se evita concentrar demasiadas responsabilidades en un solo objeto?
Antipatrón de Hardcoding	
☐	¿No se incluyen valores sensibles directamente en el código fuente?
☐	¿Se utilizan sistemas de gestión de secretos para manejar claves API y contraseñas?

Imagen [14] . Preguntas de seguridad para el desarrollo de software y las buenas prácticas - base 1.

Ministerio de Minas y Energía

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

	Antipatrón de Copy-Paste Programming
☐	¿Se evita la duplicación de código?
☐	¿Se mantiene la consistencia y se facilita la actualización del código?
	Arquitecturas Seguras
	Arquitectura de Microservicios
☐	¿Los servicios están aislados y se comunican a través de APIs?
☐	¿Se gestionan autenticación y autorización de manera centralizada mediante un gateway de API?
	Arquitectura en Capas (Layered Architecture)
☐	¿Se implementan múltiples capas de seguridad en la arquitectura?
☐	¿Cada capa añade redundancia y control de seguridad?
	Arquitectura Event-Driven
☐	¿Se utilizan colas de mensajes y brokers seguros para la comunicación entre componentes?
☐	¿Se asegura la integridad y confidencialidad de los datos en tránsito?
	Arquitectura Zero Trust
☐	¿Se verifica continuamente cada solicitud y acceso a recursos?
☐	¿No se asume confianza implícita dentro de la red?
	Prácticas de Desarrollo Seguro
	Principio de Privilegio Mínimo
☐	¿Cada componente del sistema y usuario tiene solo los permisos necesarios?
☐	¿Se revisan y ajustan regularmente los permisos para reducir la superficie de ataque?
	Ciclo de Vida de Desarrollo Seguro (SDLC)
☐	¿Se integran evaluaciones y pruebas de seguridad desde la planificación hasta el despliegue y mantenimiento?
☐	¿Se realizan revisiones de seguridad en cada fase del desarrollo?

Imagen [15] . Preguntas de seguridad para el desarrollo de software y las buenas prácticas - base 2.

Ministerio de Minas y Energía

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

	Definición de Controles de Seguridad en el Código
☐	¿Se utilizan listas blancas para validar entradas y listas negras para bloquear entradas peligrosas conocidas?
☐	¿Se asegura que los datos sensibles estén cifrados tanto en tránsito como en reposo?
	Revisiones de Código y Pruebas
☐	¿Se implementan revisiones de código por pares enfocadas en identificar vulnerabilidades de seguridad?
☐	¿Se integran herramientas de análisis estático (SAST) y dinámico (DAST) en el flujo de trabajo de CI/CD?
	Monitoreo y Respuesta a Incidentes
	Monitorización y Registro Avanzado
☐	¿Se mantiene un registro detallado de las actividades de los usuarios?
☐	¿Se configuran alertas en tiempo real para actividades sospechosas?
	Protección contra Exfiltración de Datos
☐	¿Se implementan soluciones DLP para monitorear y proteger la información sensible?
☐	¿Se aseguran todas las comunicaciones internas entre servicios?
	Seguridad en la Infraestructura
	Seguridad en la Nube
☐	¿Se implementan controles de seguridad específicos para entornos en la nube?
☐	¿Se configuran firewalls y sistemas de detección de intrusos (IDS/IPS)?
	Seguridad de Red
☐	¿Se configura la seguridad de red adecuada para prevenir accesos no autorizados?
☐	¿Se utilizan técnicas de microsegmentación para limitar el movimiento lateral?

Imagen [16] . Preguntas de seguridad para el desarrollo de software y las buenas prácticas - base 2

Para más información de la metodología que implementará el Ministerio de Minas y Energia para el desarrollo de sus aplicativos 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

Ministerio de Minas y Energía

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

gobernabilidad del Ministerio de Minas, 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 deContinuidad 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 Ministerio de Minas y Energía 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 el tercer trimestre se establece la hoja de ruta del proceso de auditoria apara los Sistemas de información SI y de los desarrollos pertinentes:

Imagen [17] . Hoja de ruta para procesos de auditoria en los SI.

Teniendo en cuenta lo anterior, se tiene en la actualidad 13 sistemas de información con módulo de auditoria (a continuación, se muestran algunos ejemplos del proceso y establecimiento de datos de los Logs, sin embargo, no se muestra la lista completa ya que es de carácter público reservado, esto con fines de confidencialidad y asuntos

Ministerio de Minas y Energía

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

internos, para más información remitirse al personal de seguridad de la información encargado).

Imagen [18] . Ejemplo de auditoria SI SISEG, listado de acceso por usuarios (los usuarios expuestos son casos de ejemplo no correspondiente a credenciales reales).

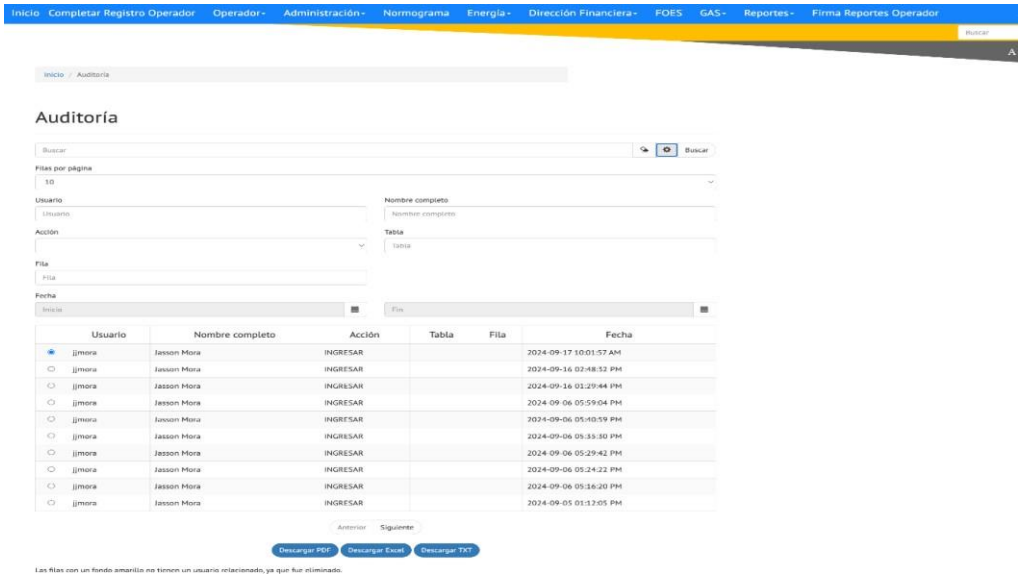


Imagen [19]. Ejemplo de auditoria SI SISEG, filtrado (los usuarios expuestos son casos de ejemplo no correspondiente a credenciales reales).

Ministerio de Minas y Energía

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

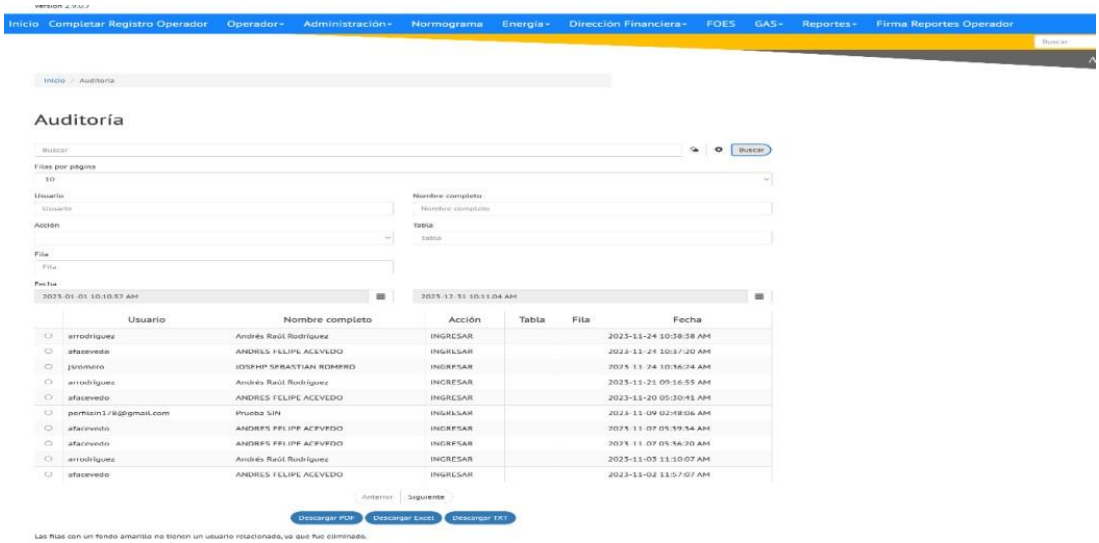


Imagen [20] . Ejemplo de auditoria SI SISEG, años anteriores (los usuarios expuestos son casos de ejemplo no correspondiente a credenciales reales).

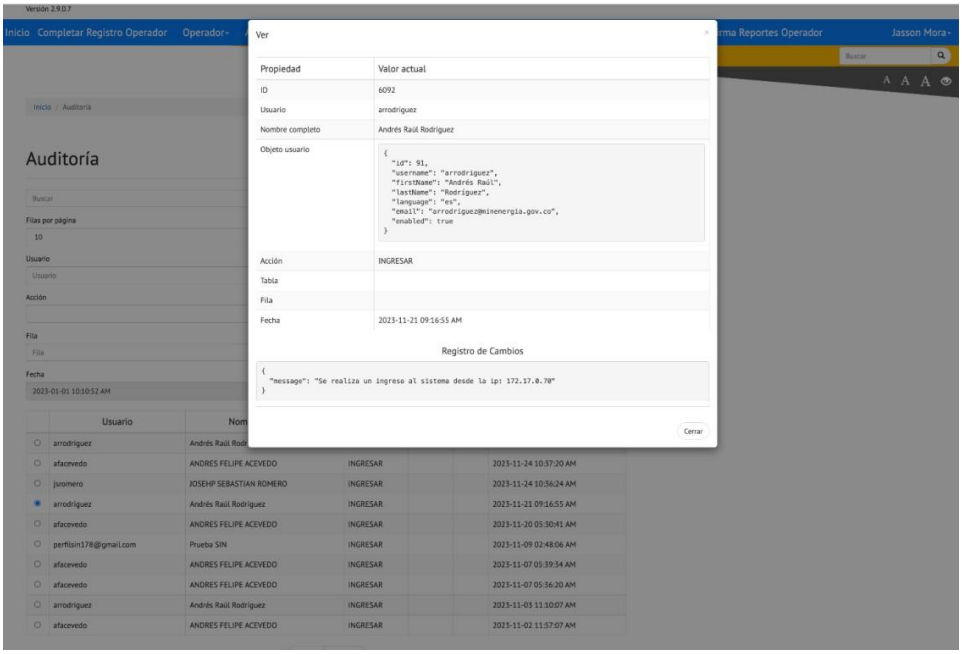


Imagen [21] . Ejemplo de auditoria SI SISEG, detalle de movimientos (los usuarios expuestos son casos de ejemplo no correspondiente a credenciales reales).

Ministerio de Minas y Energía

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

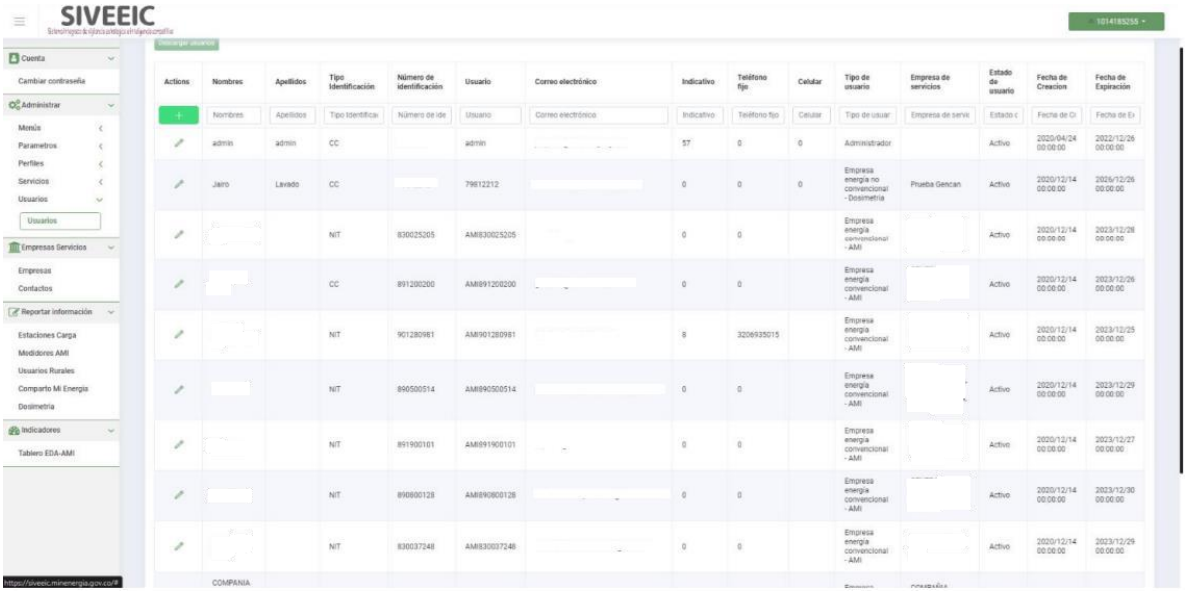


Imagen [22] . Ejemplo de auditoria SI SIVEEIC, detalle de movimientos.

Para 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.

Dicho lo anterior se muestra a continuación de 2 ejemplos de auditoria realizados con dicha herramienta:

Ministerio de Minas y Energía

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

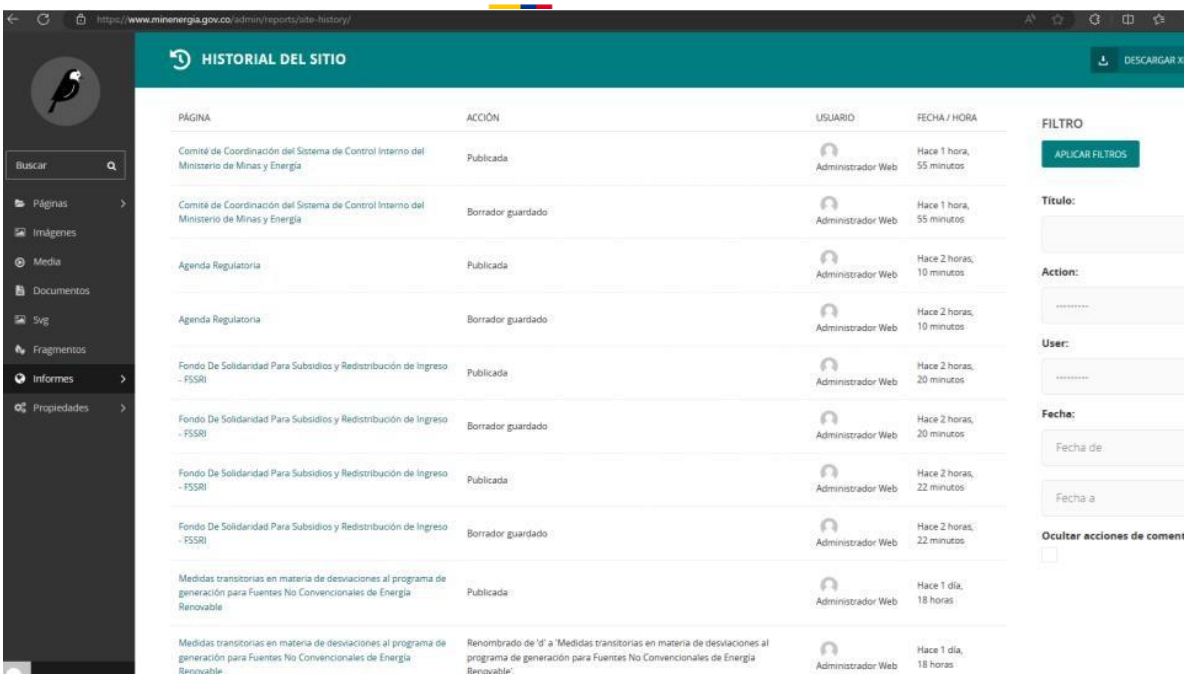


Imagen [23] . Ejemplo de auditoria SI PORTAL WEB, detalle de movimientos (los usuarios expuestos son casos de ejemplo no correspondiente a credenciales reales

Imagen [24] . Ejemplo de auditoria SI EITI Colombia, detalle de movimientos.

Ministerio de Minas y Energía

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

Es importante destacar que se debe formalizar el procedimiento de implementación del módulo de auditoría para los sistemas de información del Ministerio de Minas y Energía con herramientas óptimas y pragmáticas para mayor seguridad de los mismos e iniciar con la fase de planeación con el equipo de trabajo competente en aras de establecer una productividad conjunta en la estructuración del módulo de auditoría de los sistemasde información a los que aplique.

NOTA: Los sistemas de información anteriormente relacionados cuentan con elementos y/o componentes de auditoría no necesariamente funcionalidades específicas que sean utilizadas como módulo auditor, sin embargo, lo citado cuenta con los componentes correspondientes que evidencian el seguimiento que se realiza dentro de cada sistema.

Adicionalmente se cuenta dentro de los activos de información del Ministerio de Minas y Energía los aplicativos móviles que también poseen módulos de auditoría, a continuación, se muestra los ítems que contiene y los resultados públicos que se pueden establecer, si se desea más información de datos que pueda proveer consultar con el encargado de seguridad de la información o el equipo de desarrollo del grupo TICS.

Módulo de auditoria App Móvil Energía del Cambio:

El comportamiento de la aplicación móvil "Energía del Cambio" durante el periodo de Julio a Septiembre de la vigencia en curso, con un enfoque en los usuarios únicos diarios en Colombia. Se incluye una tabla con las estadísticas diarias y un análisis de los cambios en la cantidad de usuarios con la aplicación descargada durante el periodo.

- **Configuración del informe:**

➢ **Usuarios únicos:** Diarios.
➢ **País o región:** Colombia.
➢ **Serie temporal:** Diaria.
➢ **Usuarios con la aplicación descargada:** Todos los usuarios y usuarios únicos, analizados por intervalo.

Ministerio de Minas y Energía

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

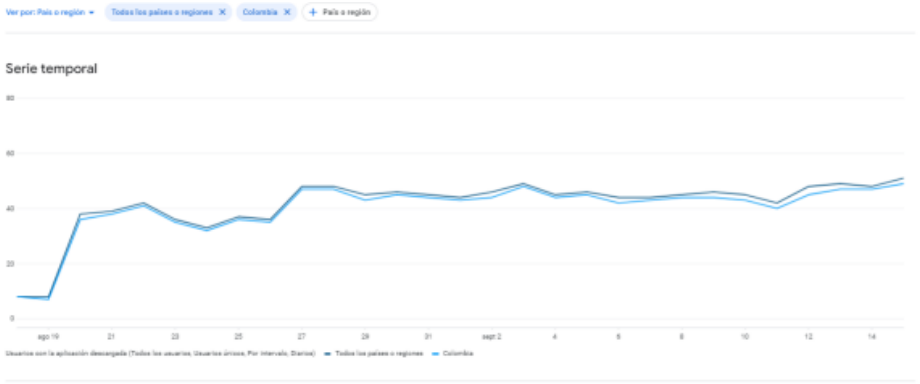


Tabla de datos:

Fecha	Usuarios Totales	Porcentaje del Total	Usuarios Únicos	Porcentaje del Total Únicos
15 de sept 2024	51	100 %	49	96,08 %
14 de sept 2024	48	100 %	47	97,92 %
13 de sept 2024	49	100 %	47	95,92 %
12 de sept 2024	48	100 %	45	93,75 %
11 de sept 2024	42	100 %	40	95,24 %
10 de sept 2024	45	100 %	43	95,56 %
9 de sept 2024	46	100 %	44	95,65 %
8 de sept 2024	45	100 %	44	97,78 %

Imagen [25] . Ejemplo de auditoria ***App Móvil Energía del Cambio***, detalle de movimientos por serie temporal y tabulación de información de ingresos y uso.

Ministerio de Minas y Energía

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

Análisis de cambios, ejemplo de contexto intervalo de tiempo definido:

Durante el periodo del 6 al 15 de septiembre de 2024, los usuarios totales con la aplicación descargada se mantuvieron relativamente estables, con una ligera variación entre los días.

A continuación, se destacan los cambios más significativos:

- **Incremento en usuarios únicos:**

Se observa un aumento constante en los usuarios únicos a lo largo del periodo, alcanzando su punto más alto el 15 de julio con 49 usuarios únicos, lo que representa un 96,08% del total de usuarios con la aplicación descargada.

- **Tendencia general:**

La cantidad de usuarios únicos se mantiene por encima del 90% del total de usuarios en la mayoría de los días. El porcentaje más bajo de usuarios únicos se registró el 12 de agosto con 93,75%.

- **Estabilidad en el uso de la aplicación:**

A lo largo de los días, el número de usuarios totales varía levemente, con un valor máximo de 51 usuarios el 15 de septiembre y un valor mínimo de 42 usuarios el 11 de septiembre.

Módulo de auditoria App Móvil "TU BOMBILLA- RETILAP"

El comportamiento de la aplicación móvil "Tu Bombilla - RETILAP" durante el periodo de julio a septiembre de la vigencia en curso, enfocándose en los usuarios únicos diarios en Colombia. Se presenta una tabla con las estadísticas diarias y se analizan los cambios en la cantidad de usuarios con la aplicación descargada durante el periodo.

- **Configuración del informe:**

➢ **Usuarios únicos**: Diarios.
➢ **País o región:** Colombia.
➢ **Serie temporal:** Diaria.

Ministerio de Minas y Energía

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

➢ **Usuarios con la aplicación descargada:** Todos los usuarios y usuarios únicos, analizados por intervalo.

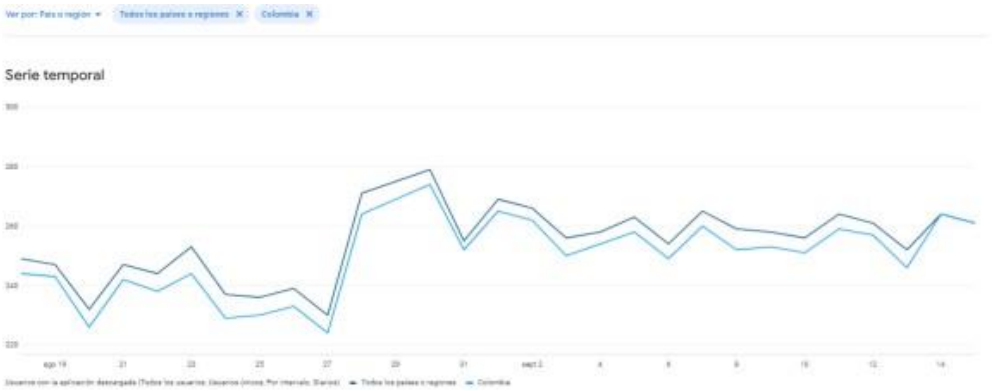


Tabla de datos:

Fecha	Usuarios Totales	Porcentaje del Total	Usuarios Únicos	Porcentaje del Total Únicos
15 de sept 2024	261	100 %	261	100 %
14 de sept 2024	264	100 %	264	100 %
13 de sept 2024	252	100 %	246	97,62 %

Imagen [26] . Ejemplo de auditoria "TU BOMBILLA -RETILAP", detalle de movimientos por serie temporal y tabulación de información de ingresos y uso.

Análisis de cambios, ejemplo de contexto intervalo de tiempo definido:

Durante el periodo de Julio a septiembre de 2024, el comportamiento de los usuarios que descargaron la aplicación "Tu Bombilla - RETILAP" presenta algunos cambios notables.

Ministerio de Minas y Energía

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

A continuación, se resaltan los puntos más significativos:

- **Incremento constante en usuarios únicos:**

A lo largo del periodo, la cantidad de usuarios únicos diarios ha sido estable, manteniéndose cercana al 100% del total de usuarios con la aplicación descargada. El porcentaje de usuarios únicos más bajo se registró el 8 de julio con un 97,3%.

- **Pico de usuarios totales:**

El número total de usuarios alcanzó un pico el 7 de septiembre de 2024, con 265 usuarios. Posteriormente, se observa una ligera disminución, alcanzando 261 usuarios el 15 de agosto.

- **Estabilidad en el uso de la aplicación:**

El número de usuarios únicos diarios también ha sido estable, manteniéndose por encima del 97% durante todo el periodo. Esto sugiere que la mayoría de los usuarios con la aplicación descargada la utilizan de manera regular.

- **Diferencias entre usuarios únicos y totales:**

La mayor diferencia entre usuarios totales y usuarios únicos se observó el 13 de septiembre, donde de los 252 usuarios totales, 246 fueron usuarios únicos, lo que representa el 97,62%.

Módulo de auditoria App Móvil "MI BOLSILLO EFICIENTE"

El comportamiento de la aplicación móvil "Mi Bolsillo Eficiente" durante el periodo de Julio a Septiembre de la vigencia en curso, con énfasis en los usuarios únicos diarios en Colombia. Se detalla una tabla con las estadísticas diarias y se realiza un análisis de los cambios observados en el número de usuarios con la aplicación descargada.

Configuración del informe:

➢ **Usuarios únicos:** Diarios.
➢ **País o región:** Colombia.
➢ **Serie temporal:** Diaria.

Ministerio de Minas y Energía

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

➢ **Usuarios con la aplicación descargada:** Todos los usuarios y usuarios únicos, analizados por intervalo diario

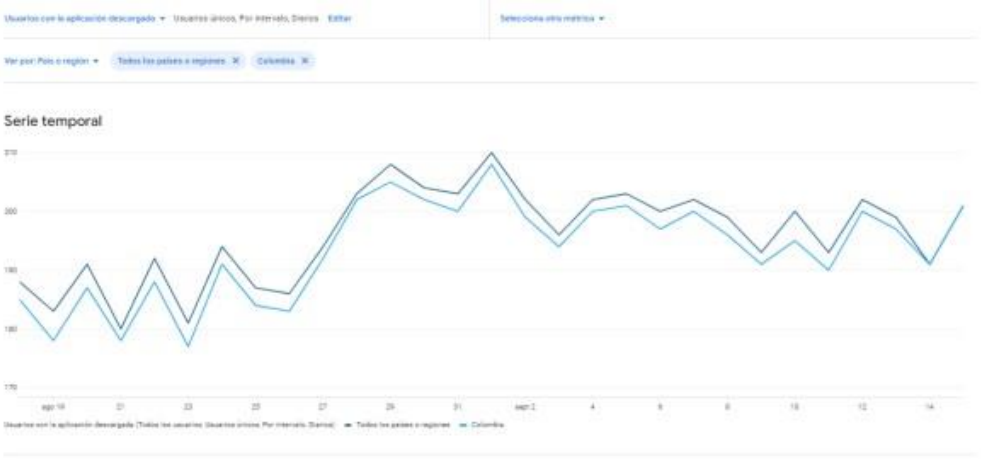


Tabla de datos:

Fecha	Usuarios Totales	Porcentaje del Total	Usuarios Únicos	Porcentaje del Total Únicos
15 de sept 2024	201	100 %	201	100 %
14 de sept 2024	191	100 %	191	100 %
13 de sept 2024	199	100 %	197	98,99 %
12 de sept 2024	202	100 %	200	99,01 %
11 de sept 2024	193	100 %	190	98,45 %
10 de sept 2024	200	100 %	195	97,5 %

Imagen [27] . Ejemplo de auditoria “MI BOLSILLO EFICIENTE”, detalle de movimientos por serie temporal y tabulación de información de ingresos y uso.

Ministerio de Minas y Energía

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

- **Análisis de cambios:**

Durante el periodo comprendido entre Julio a Septiembre de 2024, la aplicación "Mi Bolsillo Eficiente" presentó los siguientes comportamientos en cuanto a la cantidad de usuarios totales y usuarios únicos:

- **Incremento constante en usuarios totales y únicos:**

  El número de usuarios totales varió levemente durante el periodo, alcanzando un valor máximo de 202 usuarios los días 12 y 7 de julio, mientras que el número mínimo de usuarios totales fue de 191 el 14 de septiembre.

- **Alta participación de usuarios únicos:**

  A lo largo del periodo, el porcentaje de usuarios únicos se mantuvo elevado, oscilando entre el 97,5% y el 100% del total de usuarios con la aplicación descargada. El menor porcentaje de usuarios únicos se registró el 10 de septiembre con un 97,5%.

- **Estabilidad en el uso de la aplicación:**

  El comportamiento diario de los usuarios con la aplicación descargada se mantuvo estable, con ligeras variaciones en el número total de usuarios, pero con una alta proporción de usuarios únicos en todos los días analizados.

Actualmente el Ministerio de Minas y Energía cuenta con 9 SI a la cuales no se les han aplicado un módulo de auditoría, de esta manera el equipo de desarrollo del grupo TICS se encuentra en el paso cinco (5) “estado de los sistemas de información”, donde se está generando el plan de trabajo adecuado para revisar si estos faltantes tienen la necesidad de incluir dicho modulo, los lineamientos de cada frente de solución y el argumento que se debe plantear de acuerdo a la política de gobierno digital y las políticas de seguridad de la información internas de la entidad.

Ministerio de Minas y Energía

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

- **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:

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 el backup 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 remitir al responsable de seguridad de la información a cargo.

  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.

  Para el tercer trimestre se tienen identificadas las siguientes actividades en relación con el proceso de backup :

  - A comienzos de septiembre se realizó la reinstalación del appliance Arcserve Backup, cuyo sistema operativo se encontraba inaccesible. Con esta acción, se garantizó el acceso al sistema y se procedió con una exhaustiva revisión y ajuste de los procesos de respaldo (backup) para los servidores actualmente incluidos en el plan de backup. Este proceso permitió optimizar las tareas de copia de seguridad y asegurar la integridad de los datos críticos del Ministerio de Minas y Energía (MME).

Ministerio de Minas y Energía

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

- Simultáneamente, se está llevando a cabo el levantamiento de información sobre los servidores que, a la fecha, no están incorporados en el plan de backup. El objetivo es incluirlos, en la medida de lo posible, según la capacidad de la herramienta Arcserve. Este proceso es esencial para ampliar la cobertura de protección de datos y minimizar los riesgos de pérdida de información en la infraestructura del MME.

- El 20 de septiembre se lanzó un backup completo ('full backup') a cinta de toda la infraestructura. Este proceso finalizó el 27 de septiembre en horas de la noche, garantizando un respaldo integral de los datos y sistemas críticos ante cualquier evento catastrófico que pueda afectar al MME. Este respaldo es un componente esencial dentro del Plan de Recuperación ante Desastres (DRP), ya que asegura la disponibilidad de la información clave del Ministerio en caso de contingencias.

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

  En el según 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 ENERGIA en sus soluciones de hiper-convergencia, de manera que para esta etapa se debe realizar :

- Pruebas falla nodo fabric interconnect

Tabla 2 . Procesos indicados para las pruebas del datacenter

No	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 remitirse con el 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

- Informe de tercer trimestre : El 14 de septiembre, como resultado de un corte de energía programado, fue necesario llevar a cabo un apagado controlado de toda la infraestructura virtualizada en el Datacenter del MME. Posteriormente, se realizó un encendido controlado de todos los servidores, librerías, sistemas de almacenamiento y dispositivos activos de red, lo que permitió asegurar que todos los servicios y aplicaciones alojados en esta infraestructura se reiniciaran correctamente. Este procedimiento fue fundamental para garantizar la continuidad operativa de los servicios del Ministerio de Minas y Energía sin interrupciones.

- Por último, se ha programado el mantenimiento físico de los servidores en el Datacenter principal para el viernes XX de octubre. Este mantenimiento busca optimizar el rendimiento físico de los servidores y asegurar su adecuado funcionamiento, prolongando su vida útil y minimizando posibles fallas futuras en la infraestructura tecnológica del Ministerio.

- 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.

Para el tercer trimestre se establece la guía formal de cifrado mediante nuestro proveedor de antivirus el cual es Kapersky, a partir de ello el documento estipula lo siguiente:

1. **Guía metodológica y aspectos clave de cifrado de unidades extraíbles :**

“Este componente está disponible si Kaspersky Endpoint Security se instala en un equipo con Windows para estaciones de trabajo. Este componente no está disponible si Kaspersky Endpoint Security está instalado en un equipo con Windows para servidores. Admite el cifrado de archivos en los sistemas de archivos FAT32 y NTFS. Si una unidad extraíble con un sistema de archivos no compatible está conectada al equipo, la tarea de cifrado de esta unidad extraíble finaliza con un error y asigna el estado de solo lectura a la unidad extraíble”

2. **Tipos de cifrado:**

Ministerio de Minas y Energía

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

- **Cifrado de disco completo (FDE)** :
  Donde se cifra toda la unidad extraíble, incluido el sistema de archivos y hay que tener en cuenta lo siguiente: *“No se puede acceder a datos cifrados fuera de la red corporativa. También es imposible acceder a datos cifrados dentro de la red corporativa si el equipo no está conectado a Kaspersky Security Center (p. ej., en un equipo "invitado").”*
- **Cifrado de archivos (FLE):**
  Donde se cifra solo los archivos de la unidad extraíble, el sistema de archivos permanece sin cambios lo que permite que se pueda estar en “modo portátil” fuera de la red corporativa, en este Kapersky Endpoint Security genera una clave maestra y la guarda en su servidor central, en el equipo del usuario y en la unidad extraíble, esta clave está cifrada con la clave publica del software.

3. **Acceso a datos cifrados:**

Procedimiento de acceso y protocolo mediante el software, de manera que se revisa si hay clave maestra dentro del equipo, en caso de que no exista se procede a la petición al servidor del proveedor, posteriormente se tiene el descifrado de datos el cual dependerá de los equipos administrados y del contexto de la unidad (si son solo de lectura, ejecución ,etc)

4. **Características especiales del cifrado de unidades extraíbles :**

Es importante destacar que las unidades extraíbles (medios conectados por medio de USB, discos duros por USB o FireWire o unidades SSD) estarán sujetas al contexto del equipo donde planea hacer el proceso de cifrado, el cual debe estar debidamente configurado y estar en lista de los equipos administrados del servidor de Kapersky Security Center. Además, es importante resaltar que dicho software no cifra ni descifra archivos de solo lectura ya que están sujetos a los permisos que ha adquirido antes dicho activo de información.

5. **Proceso paso a paso de cifrado de archivos:**

En este se establece la guía que se debe llevar para el cifrado correcto de los archivos, manteniendo condiciones que se pueden dar durante el proceso, este consta de 12 pasos para que logre hacer de forma íntegra y efectiva. (Para mayor información de la guía, remitirse a la mesa de ayuda del grupo TICS).

Ministerio de Minas y Energía

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

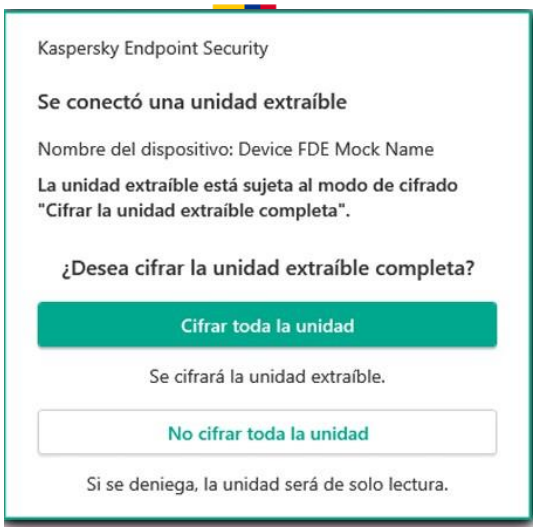


Imagen [28] . Solicitud de cifrado para una unidad extraíble.

En caso de no optar con el software y se requiera cifrar el archivo en otro dispositivo, el proveedor posee un ejecutable denominado “Gestor de archivos portatil” el cual proporciona una interfaz para trabajar los archivos y el cual almacena una clave cifrada con la contraseña del usuario.

6. **Proceso paso a paso de descifrado de archivos :**

   Como en el punto anterior también se establece la guía que se debe llevar para descifrado de archivos, este consta de 8 pasos y también esta generado a partir de las condiciones del usuario y sus dispositivos, es importante destacar que este proceso dependerá del establecimiento de las reglas de cifrado-descifrado de la unidad extraíble.

Dicho lo anterior, se establece un proceso de cifrado y descifrado utilizando un software especializado que ha sido autorizado por el Ministerio de Minas y Energía. Este software es “BitLocker”, una herramienta de cifrado de disco completo que viene integrada en los sistemas operativos de “Windows” de Microsoft.

La guía oficial del Ministerio detalla un procedimiento en 11 pasos para que los usuarios puedan utilizar correctamente BitLocker. Estos pasos incluyen la activación del cifrado, la configuración de las políticas de seguridad, y las instrucciones para recuperar datos en caso de pérdida de credenciales o fallos del sistema. Además, la guía ofrece un contexto adicional sobre qué hacer en caso de tener dispositivos que no cuenten con BitLocker preinstalado, proporcionando

Ministerio de Minas y Energía

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

recomendaciones de soluciones alternativas o cómo instalar el software en sistemas compatibles. (Para mayor información de la guía, remitirse a la mesa de ayuda del grupo TICS).

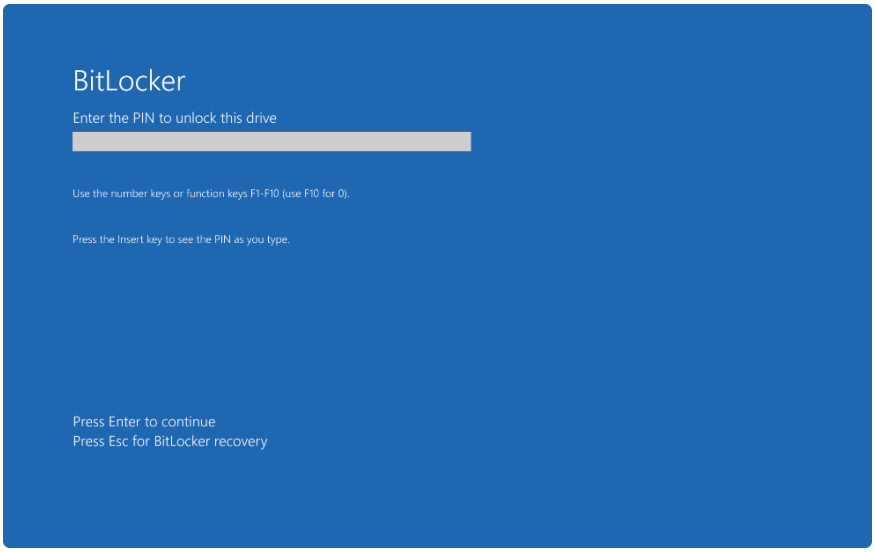


Imagen [29] . interfaz de Bitlocker para descifrado de archivos.

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 (abril, mayo y junio) que conlleva el seguimiento del plan de seguridad y privacidad de la información y la gestión de riesgos TIC.

A partir de lo anterior se hace seguimiento según frecuencia de auditoria que implica el tercer trimestre (julio, agosto y septiembre) se realiza edición de la documentación del informe del plan de seguridad y privacidad de la información con miras de anexar continuidad de guias de cifrado, auditoria de SI actualizados, configuraciones y pruebas de FW y antivirus, requerimientos de Aranda y pruebas realizadas de mantenimiento, backups y sensibilización de acuerdo a cronograma.

Ministerio de Minas y Energía

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

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:

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

No	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

A partir del cronograma y entendiendo las fechas e intervalos de tiempo determinados para el tercer trimestre se tiene el siguiente resultado de incidentes de seguridad:

- Se ha identificado un incidente crítico en el cual se comprometieron credenciales de acceso pertenecientes al dominio del Ministerio de Minas y Energía. Estas credenciales fueron encontradas a la venta en la deep web, lo que representa una amenaza significativa para la seguridad de los sistemas de información del ministerio.

Ministerio de Minas y Energía

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

Ante este hallazgo, se activó de inmediato el plan de gestión de incidentes, en coordinación con el equipo de mesa de ayuda y el grupo TICs. Como primera medida, se procedió a la inhabilitación de las credenciales comprometidas, además de notificar a todas las partes involucradas para realizar una revisión exhaustiva del contexto y evaluar los posibles sistemas de información comprometidos.

Adicionalmente, se incrementó el monitoreo de anomalías o eventos sospechosos, ya que existe la posibilidad de que se haya producido una intrusión no autorizada con movimiento lateral dentro de la red del ministerio. Esto implica que los atacantes podrían haber obtenido acceso a otros sistemas internos. Actualmente, se está llevando a cabo un proceso de monitoreo continuo para identificar cualquier comportamiento inusual y mitigar futuros riesgos. (si se desea saber mayor información del incidente se debe remitir con el oficial de seguridad de la información a cargo)

A partir de lo mencionado anteriormente, se ha recibido retroalimentación y, en el marco de la mejora continua, se ha definido la actividad número 3, titulada 'Inicio de los cambios necesarios a las políticas y procedimientos de seguridad'. En esta etapa, se establece la actualización del proceso, el normograma y el flujo de procesos del 'Procedimiento de Gestión de Incidentes de Seguridad de la Información'.

Este procedimiento se encuentra actualmente en la actividad número 4, denominada 'Aprobar las políticas de seguridad', donde se validarán las modificaciones propuestas. Se espera que para el cuarto trimestre del año, y siguiendo el cronograma establecido junto con la asignación de responsabilidades, el proceso sea formalmente difundido.

Junto con este proceso, también se difundirá el documento **'T-GT-F-05 FORMATO REPORTE DE INCIDENTES'**, el cual ha sido verificado por los responsables de seguridad de la información del Ministerio de Minas y Energía. Dicho formato ha sido diseñado y aprobado para cumplir con las características necesarias en el proceso de gestión de incidentes de seguridad,abarcando tanto riesgos cibernéticos como aspectos relacionados con la infraestructura crítica del Ministerio.

Ministerio de Minas y Energía

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

Energía	FORMATO REPORTE DE INCIDENTES	SIG Sistema Integrado de Gestion del Minenergía
		T-GT-F-06
		26-07-2023 | V-3

DATOS DE LA PERSONA QUE NOTIFICA			
NOMBRE:		DEPENDENCIA:	
INFORMACIÓN SOBRE EL INCIDENTE			
FECHA DEL INCIDENTE:	HORA POSIBLE:	DURACIÓN DEL INCIDENTE:	
Marque con una X las opciones que considere aplicables a la pérdida de la continuidad en los procesos:			
☐	Ocasionada por adulterar, eliminar, o acceder a información sensible o secreta.	☐	Por eventos naturales.
☐	Ocasionada por deficiencias en gestión de personal crítico y administración del conocimiento especializado del área.	☐	Por modificación no autorizada de un sitio o página web.
☐	Por suspensión de servicios suministrados por proveedores críticos externos.	☐	Por atentados.
☐	Por Insuficientes condiciones de seguridad en los procesos.	☐	Por modificación o eliminación no autorizada de datos.
☐	Por detención de aplicaciones y servicios críticos ofrecidos por Tecnología de la Información.	☐	Por Anomalía o vulnerabilidad técnica de software.
☐	Por Ausencia de Planes Alternos de Operación o deficiencias en los mismos.	☐	Por debilidades o inexistencia del esquema de recuperación tecnológica.
☐	Interrupción prolongada en un servicio de red.	☐	Por Ataque o infección por código malicioso (virus, gusanos, troyanos, etc.).
☐	Por Imposibilidad de ingresar a las instalaciones físicas.	☐	Por robo o pérdida de un recurso informático crítico.
☐	Por cese de actividades.	☐	Otro no contemplado. (diligencie en descripción del incidente)
DESCRIPCIÓN DEL INCIDENTE:			

Imagen [30] . Formato reporte de gestión de incidentes – Incidentes relacionados con riesgos de seguridad y privacidad de la información.

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 MME.

Para el tercer trimestre se dispone el siguiente análisis que parte de aspectos generales que se tiene sobre las tecnologías de la información y la normatividad que se exige por parte del Ministerio de Minas y Energía y en cumplimiento a los requerimientos que parte de normas internacionales sobre seguridad y privacidad de la información:

El sector de las tecnologías de la información y comunicaciones (TIC) ha experimentado avances constantes que impactan directamente en la evolución de soluciones tecnológicas, mejorando las funcionalidades y capacidades tanto del hardware como del software. Estos avances han permitido optimizar la eficiencia y velocidad en el procesamiento de la información, lo que se traduce en un aumento significativo de la productividad económica. En Colombia, programas como el de Fortalecimiento de la Industria TI (FITI) del Ministerio de las TIC y el Programa de Transformación Productiva (PTP) del Ministerio de Industria, Comercio y Turismo

Ministerio de Minas y Energía

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

han reconocido este sector como estratégico para el país, impulsando su crecimiento y desarrollo.

En los últimos tres años, el gobierno colombiano ha invertido más de 350 mil millones de pesos en la modernización de sus tecnologías de la información, lo que ha mejorado su actividad y niveles de servicio en un 43%. Las TIC no solo han sido un motor de crecimiento económico comparable a sectores tradicionales como la construcción, sino que también han facilitado el surgimiento de nuevos segmentos educativos, respondiendo a la creciente demanda de profesionales y técnicos en todos los estratos socioeconómicos. Este impulso tecnológico ha generado empleo, promovido la exportación de mano de obra calificada y contribuido a la financiación de otros sectores económicos.

A pesar de los avances, el acceso a la información pública sigue siendo un desafío debido a los costos asociados a la infraestructura y los recursos necesarios para garantizar la disponibilidad oportuna de los datos. La mayoría de la información estatal es pública, pero la inversión en tecnologías adecuadas es vital para que las entidades gubernamentales mantengan sus sistemas a la vanguardia y respondan a las nuevas exigencias del mercado. Esto se refleja en la creciente adopción de tecnologías avanzadas para optimizar la interacción con los ciudadanos y mejorar la eficiencia en la gestión de la información.

A nivel global, las TIC han contribuido de manera significativa al bienestar social, ayudando a reducir las brechas sociales y generando externalidades positivas en la mayoría de los sectores productivos. La difusión del internet ha democratizado el acceso al conocimiento, y la convergencia de servicios de telefonía, televisión y transmisión de datos ha sido clave en este proceso. La sociedad ha migrado hacia una era de la información, donde la conectividad y la accesibilidad son elementos fundamentales para el desarrollo social y económico.

Finalmente, el sector de las TIC en Colombia ha mostrado rendimientos positivos gracias a la innovación constante y al crecimiento exponencial que se vive en los mercados tecnológicos globales. La implementación de sistemas que optimizan procesos y recursos es cada vez más común, y se ha vuelto más accesible y rentable para las empresas. Esto demuestra cómo las tecnologías se han consolidado como un pilar fundamental en el desarrollo económico y social del país, impulsando tanto el sector público como el privado hacia nuevas fronteras de eficiencia y modernización.

En respuesta a los avances tecnológicos y la evolución de los componentes disruptivos de la Cuarta Revolución Industrial, el gobierno colombiano, a través del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), ha redefinido su enfoque estratégico hacia dos áreas clave: la Política de Gobierno Digital y la Política de Seguridad Digital. Estas directrices buscan fomentar la transformación digital en todos los sectores, abarcando tanto entidades públicas como el sector privado, la academia y la ciudadanía en general. El objetivo principal

Ministerio de Minas y Energía

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

es integrar las actividades de producción de bienes y servicios dentro del ámbito digital, promoviendo la eficiencia y modernización en todos los frentes.

El marco normativo que rige el sector TIC en Colombia es amplio y comprende diversas leyes y decretos que regulan y protegen tanto la propiedad intelectual como el uso de la tecnología y los datos personales. Algunas de las normativas más relevantes incluyen:

- **Ley 603 de 2000**: Protección de los derechos de autor en Colombia, incluyendo el software como activo protegido.
- **Ley 842 de 2003**: Reglamentación del ejercicio de la ingeniería, afines y profesiones auxiliares, aplicable a actividades del sector TIC.
- **Ley Estatutaria 1266 de 2008**: Disposiciones sobre el Hábeas Data y regulación del manejo de bases de datos personales.
- **Decreto Ley 1273 de 2009**: Modificaciones al Código Penal relacionadas con la confidencialidad y disponibilidad de datos y sistemas informáticos.
- **Ley 1273 de 2009**: Creación de un nuevo bien jurídico para la protección de la información y los datos, con sanciones para los atentados informáticos.
- **Ley 1341 de 2009**: Definición de los principios para la organización de las Tecnologías de la Información y las Comunicaciones (TIC), y la creación de la Agencia Nacional del Espectro.
- **Ley Estatutaria 1581 de 2012**: Protección de datos personales, con directrices para entidades públicas y privadas sobre el manejo de dichos datos.
- **Decreto 1377 de 2013**: Reglamentación parcial de la Ley 1581 de 2012, enfocada en la protección de datos personales.
- **Plan Plurianual de Inversiones 2018-2022**: "Pacto por Colombia, pacto por la equidad".
- **Resolución 00500 de 2021**: Establecimiento de lineamientos para la estrategia de seguridad digital y adopción del Modelo de Seguridad y Privacidad de la Información (MSPI).
- **CONPES 3995 de 2020**: "Política Nacional de Confianza y Seguridad Digital".
- **Ley 1978 de 2019**: Modernización del sector TIC, distribución de competencias y creación de un regulador único.
- **CONPES 3975 de 2019**: "Política Nacional de Transformación Digital e Inteligencia Artificial".

Ministerio de Minas y Energía

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

Estas leyes y normativas proporcionan un marco legal sólido que permite el desarrollo y la implementación de tecnologías de la información en Colombia, promoviendo la seguridad y el acceso equitativo a la tecnología en todos los sectores. Con ellas, el país se prepara para los retos tecnológicos actuales, apoyando la transformación digital de la economía y la sociedad.

Teniendo en cuenta el contexto mencionado anteriormente y tras realizar un análisis exhaustivo de los riesgos que actualmente enfrenta el Ministerio de Minas y Energía, resulta evidente la necesidad de reforzar sus capacidades de protección cibernética. Los riesgos identificados son transversales a los activos de información que maneja la entidad, incluyendo datos sensibles relacionados con la infraestructura energética, proyectos estratégicos, investigaciones, y comunicaciones que pueden ser objeto de ciberataques o amenazas internas y externas.

En este contexto, se ha identificado como una prioridad la **"Adquisición, instalación y puesta en funcionamiento de una solución de ciberdefensa para el monitoreo y detección de amenazas en tiempo real para la Red del Ministerio de Minas y Energía (MINENERGIA)"**. Esta solución permitirá garantizar la integridad, disponibilidad, y confidencialidad de la información gestionada por la entidad, fortaleciendo su postura frente a las crecientes amenazas cibernéticas que afectan tanto al sector público como al privado.

La implementación de esta solución es fundamental, no solo para asegurar la protección de los sistemas internos del Ministerio, sino también para garantizar la continuidad operativa de los procesos relacionados con la **gestión energética del país**, un sector clave para el desarrollo económico y la seguridad nacional. Dado que la información manejada incluye aspectos de vital importancia para la seguridad energética y la estabilidad del país, cualquier incidente de seguridad podría tener repercusiones significativas, tanto a nivel operativo como estratégico.

Finalmente, esta iniciativa se alinea con las políticas nacionales de seguridad digital y ciberdefensa, permitiendo al Ministerio de Minas y Energía cumplir con los estándares internacionales y nacionales en materia de ciberseguridad. Esto posicionará a la entidad en un marco de resiliencia frente a los ataques cibernéticos, mientras fortalece la confianza en sus sistemas y protege los activos críticos de información que son esenciales para el bienestar y progreso del país.

El objetivo principal de esta solución de **ciberdefensa** será el establecimiento de un sistema integral de monitoreo de la red, capaz de detectar de manera proactiva amenazas y vulnerabilidades antes de que puedan comprometer los sistemas críticos. Esta plataforma debe contar con capacidades avanzadas para identificar actividades sospechosas en tiempo real, permitir la respuesta rápida ante incidentes, y facilitar la adopción de medidas preventivas a través del análisis continuo de riesgos, de esta manera se establecen las siguientes características:

Ministerio de Minas y Energía

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

- Detección de amenazas.
- Visualización de RED.
- Visibilidad de amenazas.
- Arquitecturas de solución.
- Notificaciones en tiempo real.
- Administración.
- Contención (en soluciones de SandBox).
- Periodo de vigencia.
- Soporte.
- Gestión y administración de operaciones de seguridad tipo SOC.
- Cursos certificados.

La gestión de esta actividad se encuentra en su fase final de cierre. Actualmente, se cuenta con varios oferentes que han presentado soluciones robustas y alineadas con el presupuesto establecido para el proyecto. Se proyecta que, durante el cuarto trimestre, se establezcan los requerimientos técnicos necesarios para la implementación sobre la infraestructura tecnológica actual del Ministerio de Minas y Energía, garantizando el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) pactados con el proveedor seleccionado.

Para obtener información adicional sobre este proceso dirigirse al coordinador(a) del grupo TIC, ya que el contenido es de carácter confidencial. Este seguimiento únicamente detalla los aspectos públicos relacionados con la actividad.

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.

Ministerio de Minas y Energía

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

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 cambia constantemente y aun es habitual que muchos 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

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

No	Grupo objetivo
1	OFICINA ASESORA DE JURIDICA
2	Grupo de Coordinación Interinstitucional y Seguimiento de Fallos
3	Grupo de Energía Eléctrica
4	Grupo de Hidrocarburos

Ministerio de Minas y Energía

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

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 PLANEACION Y GESTION 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	SUBDIRECCION 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	DIRECCION DE FORMALIZACION 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	DIRECCION DE MINERIA EMPRESARIAL
27	Grupo de Ejecución Y Gestión Minera
28	Grupo de Formulación de Política Y Reglamentación Minera
29	Grupo de Planeación Y Seguimiento Minero
30	DIRECCION DE HIDROCARBUROS
31	Grupo de Gas Combustible
32	Grupo de Gestión de Proyectos Y Optimización
33	Grupo Downstream
34	Grupo Midstream
35	Grupo Upstream

Ministerio de Minas y Energía

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

Para el tercer trimestre y siguiendo la hoja de ruta se logró la implementación de dicho gestor de contraseñas para 10 grupos objetivo de acuerdo con la siguiente lista:

Tabla 5. Grupos objetivo para la implementación de gestor de contraseñas tercer trimestre 2024

No	Grupo objetivo
1	Grupo de asuntos legislativos
2	Grupo de regalías
3	Oficina de asuntos ambientales y sociales
4	Grupo de gestión ambiental
5	Oficina de asuntos regulatorios y empresariales
6	Grupo de asuntos nucleares
7	Grupo de política y regulación energética
8	Oficina de control disciplinario interno
9	Oficina de control interno
10	Grupo de relacionamiento con el ciudadano y gestión de la información

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.

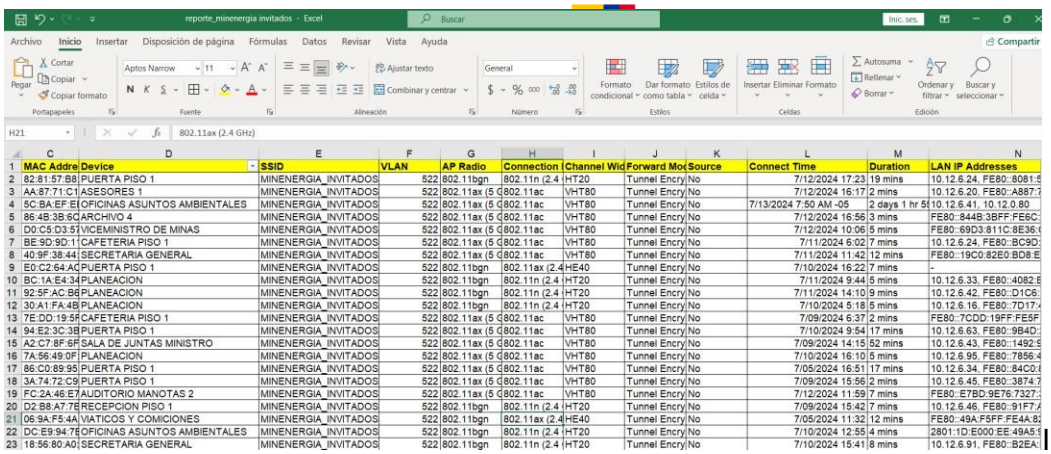
Estas solicitudes de registro deben ser aprobadas por los anfitriones (funcionarios o contratistas) registrados en el directorio activo y tiene entre otras políticas la restricción de navegación en páginas potencialmente peligrosas.

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



MAC Addre	Device	SSID	VLAN	AP Radio	Connection	Channel Wid	Forward Mo	Source	Connect Time	Duration	LAN IP Addresses
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
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
5C:BA:EF:E(	OFICINAS ASUNTOS AMBIENTALES	MINENERGIA_INVITADOS	522	802.11ac	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
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:
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:
BE:9D:9D:11	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:
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
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	-
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
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:
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
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:
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:
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
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
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::84C0:6
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
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:
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
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
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:49A5:1
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:1

Imagen [31] . Formato de informe del acceso al portal cautivo del MME 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 es de vital importancia para poder definir las siguientes características:

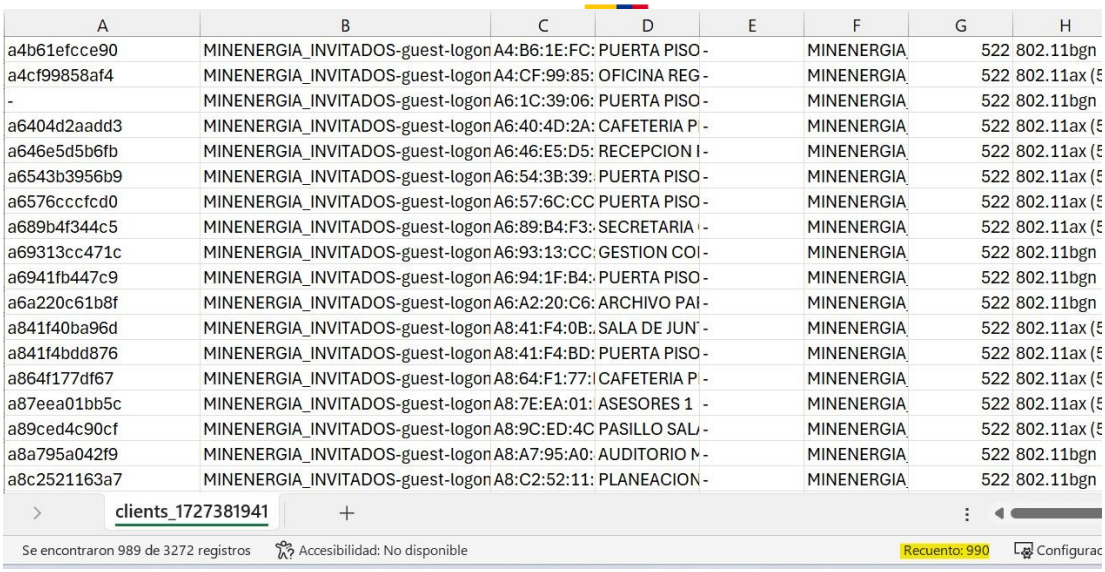
1. **Punto de conexión más usado:** Oficina de planeación
2. **VLAN de conexión**
3. **Dirección IP de acceso**
4. **MAC del dispositivo**
5. **Tiempo de conexión**

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.

Durante el tercer semestre, se registraron un total de **990 conexiones** a la red WiFi de visitantes a través del portal cautivo del Ministerio de Minas y Energía. Este número refleja un incremento significativo en las sesiones, lo que permite concluir que el proceso de conexión mediante el dominio **@minenergia.gov.co** se está ejecutando de manera correcta y controlada para la mayoría de los usuarios.

Ministerio de Minas y Energía

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



A	B	C	D	E	F	G	H
a4b61efcce90	MINENERGIA_INVITADOS-guest-logon	A4:B6:1E:FC:	PUERTA PISO	-	MINENERGIA	522	802.11bgn
a4cf99858af4	MINENERGIA_INVITADOS-guest-logon	A4:CF:99:85:	OFICINA REG	-	MINENERGIA	522	802.11ax (5
-	MINENERGIA_INVITADOS-guest-logon	A6:1C:39:06:	PUERTA PISO	-	MINENERGIA	522	802.11bgn
a6404d2aadd3	MINENERGIA_INVITADOS-guest-logon	A6:40:4D:2A:	CAFETERIA P	-	MINENERGIA	522	802.11ax (5
a646e5d5b6fb	MINENERGIA_INVITADOS-guest-logon	A6:46:E5:D5:	RECEPCION I	-	MINENERGIA	522	802.11ax (5
a6543b3956b9	MINENERGIA_INVITADOS-guest-logon	A6:54:3B:39:	PUERTA PISO	-	MINENERGIA	522	802.11ax (5
a6576cccfcd0	MINENERGIA_INVITADOS-guest-logon	A6:57:6C:CC	PUERTA PISO	-	MINENERGIA	522	802.11ax (5
a689b4f344c5	MINENERGIA_INVITADOS-guest-logon	A6:89:B4:F3:	SECRETARIA	-	MINENERGIA	522	802.11ax (5
a69313cc471c	MINENERGIA_INVITADOS-guest-logon	A6:93:13:CC:	GESTION COI	-	MINENERGIA	522	802.11bgn
a6941fb447c9	MINENERGIA_INVITADOS-guest-logon	A6:94:1F:B4:	PUERTA PISO	-	MINENERGIA	522	802.11bgn
a6a220c61b8f	MINENERGIA_INVITADOS-guest-logon	A6:A2:20:C6:	ARCHIVO PAI	-	MINENERGIA	522	802.11bgn
a841f40ba96d	MINENERGIA_INVITADOS-guest-logon	A8:41:F4:0B:	SALA DE JUN	-	MINENERGIA	522	802.11ax (5
a841f4bdd876	MINENERGIA_INVITADOS-guest-logon	A8:41:F4:BD:	PUERTA PISO	-	MINENERGIA	522	802.11ax (5
a864f177df67	MINENERGIA_INVITADOS-guest-logon	A8:64:F1:77:	CAFETERIA P	-	MINENERGIA	522	802.11ax (5
a87eea01bb5c	MINENERGIA_INVITADOS-guest-logon	A8:7E:EA:01:	ASESORES 1	-	MINENERGIA	522	802.11ax (5
a89ced4c90cf	MINENERGIA_INVITADOS-guest-logon	A8:9C:ED:4C	PASILLO SAL	-	MINENERGIA	522	802.11ax (5
a8a795a042f9	MINENERGIA_INVITADOS-guest-logon	A8:A7:95:A0:	AUDITORIO M	-	MINENERGIA	522	802.11bgn
a8c2521163a7	MINENERGIA_INVITADOS-guest-logon	A8:C2:52:11:	PLANEACION	-	MINENERGIA	522	802.11bgn

clients_1727381941

Se encontraron 989 de 3272 registros Accesibilidad: No disponible Recuento: 990 Configurac

Imagen [32] . Formato de informe del acceso al portal cautivo del MME con información comprendida del tercer trimestre año 2024- ejemplo de datos, no corresponde al real

Sin embargo, se han identificado algunos fallos en las conexiones de aquellos usuarios que han cambiado recientemente su contraseña de acceso. Esto sugiere que el portal cautivo no está actualizando la información de credenciales de manera eficiente, lo cual está generando dificultades en la autenticación.

Para resolver esta situación, se recomienda revisar y ajustar los mecanismos de sincronización entre el sistema de autenticación de usuarios y el portal cautivo, con el fin de garantizar que los cambios de contraseña se reflejen de inmediato y asegurar una experiencia de conexión fluida y sin interrupciones.

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

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

Ministerio de Minas y Energía

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

- **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:

Ministerio de Minas y Energía

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

Tabla 6 . Pruebas de vulnerabilidades ejecutadas segundo trimestre año 2024

No	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	

Para el tercer trimestre del año 204 se continua con el proceso según cronograma y criticidad de activos de información de esta manera se tienen las siguientes actividades ejecutadas:

Tabla 7 . Pruebas de vulnerabilidades ejecutadas tercer trimestre año 2024

No	Activo objetivo	Fecha de ejecución	Resultado
1	GEOSERVER https://geoserver.minenergia.gov.co/geoserver/web/	24/07/2024	Confidencial
2	SISEGDH https://sisegdh.minenergia.gov.co/	25/07/2024	
3	SERVIDOR (172.XX.X.XXX) https://powerbi.minenergia.gov.co/	26/07/2024	
4	SISEG: https://siseg.minenergia.gov.co/	29/07/2024	
5	JASPER:	29/07/2024	

Ministerio de Minas y Energía

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

	https://jasperreport.minenergia.gov.co:8080/jasperserver/login.html	
6	GEOVISOR https://geovisor.minenergia.gov.co/visor-ide-me/	29/07/2024
7	DECLARAGAS https://declaragas.minenergia.gov.co/login.aspx	12/08/2024
8	Análisis de vulnerabilidades enfocadas a credenciales de acceso dispuestas a la venta en la DeepWeb	23/08/2024
9	Análisis de acceso de sesiones sospechosas	23/08/2024
10	AULA VIRTUAL	26/08/2024
11	GEONETWORK	28/08/2024
12	ARGO	28/08/2024
13	NORMATIVAME	17/09/2024
14	Sistema SIVEEIC https://siveeic.minenergia.gov.co/#/auth/login	18/09/2024
15	EITI	18/09/2024
16	AVANZAME https://avanzamepruebas.minenergia.gov.co/	18/09/2024
17	Portal WEB del MME	20/09/2024

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 MME, para que pueda analizarse, evaluarse y mitigarse (si es necesario). El posterior seguimiento de este proceso será el paso siguiente con el fin de encontrar resultados beneficiosos que conlleven a subsanar las vulnerabilidades y ser sometidas nuevamente a un re-test.

Durante el tercer trimestre de 2024, se realizó un seguimiento exhaustivo del proceso de subsanación de las vulnerabilidades identificadas previamente. Se adjuntan las evidencias correspondientes, incluyendo los correos de seguimiento donde se solicitó formalmente el re-test para validar las correcciones aplicadas.

Es importante resaltar que, aunque las vulnerabilidades detectadas fueron expuestas y mitigadas, el entorno digital es dinámico, lo que implica que pueden surgir nuevas vulnerabilidades que podrían ser aprovechadas por actores maliciosos en futuros ciberataques.

A partir de un nuevo análisis realizado, se identificaron sistemas de información que requieren subsanaciones adicionales en sus procesos de desarrollo (para mayor información remitirse al encargo de seguridad de la información). Estos sistemas serán sometidos a un ciclo de escaneos de seguridad periódicos para asegurar que las nuevas vulnerabilidades sean

Ministerio de Minas y Energía

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

detectadas y corregidas de manera oportuna. Este enfoque de escaneo recurrente garantiza un monitoreo continuo y una respuesta proactiva ante posibles amenazas, alineado con las mejores prácticas en ciberseguridad.

Se recomienda implementar una estrategia de mejora continua para abordar no solo las vulnerabilidades ya conocidas, sino también para anticiparse a nuevas amenazas emergentes, asegurando así la protección integral de los activos de información del Ministerio.

Imagen [33] . Formato de comunicación a dependencias sobre informes de vulnerabilidades, los datos son modo de ejemplo no corresponden a un caso real.

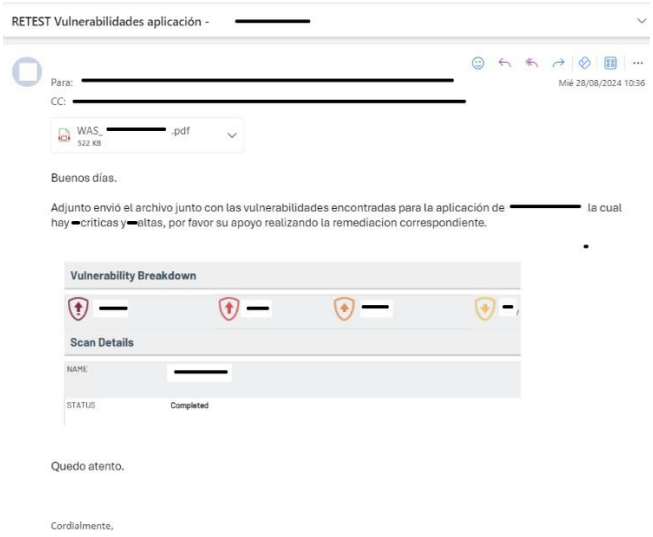


Imagen [34] . Formato de comunicación a dependencias sobre retest y seguimiento-. los datos son modo de ejemplo no corresponden a un caso real.

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.

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

Tabla 8. Cronograma de ejecución de pruebas de vulnerabilidades cuarto trimestre.

No	Fase	Actividad	Fecha
1	Preparación	Identificación de información objetivo	Mes 10 semana 2
		Definición de alcance y objetivos	Mes 10 semana 3
2	Análisis	Escaneo de vulnerabilidades (Definición y ejecución de herramienta interna o evaluación por terceros) para identificar posibles vulnerabilidades	Mes 11 semana 1
		Análisis de configuraciones (red y software)	Mes 11 semana 2
		Enumeración de servicios más expuestos	Mes 11 semana 3
3	Explotación	Pruebas de pentesting (internas o por terceros), definiendo controles de acceso (caja negra, gris o blanca) según prioridad.	Mes 12 semana 1 y 2
		Análisis de impacto	Mes 12 semana 3
4	Informe y documentación	Documentación de hallazgos	Por definir
		Recomendación de mitigación	Por definir
		Presentación del informe	Por definir
5	Implementación	Ejecutar acciones de remediación a las vulnerabilidades detectadas.	Por definir
		Ejecutar pruebas de re-test para verificar que efectivamente se hayan cerrado las vulnerabilidades.	Por definir

5.2.2 Ventanas de mantenimiento efectuadas

A partir de los hallazgos de los sistemas de información y en alineación a la normatividad el MME 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

Ministerio de Minas y Energía

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

vulnerabilidades correspondientes, de esta manera, para el segundo trimestre del año 2024 se efectuaron las siguientes actualizaciones:

Tabla 9. Ventanas de mantenimiento a herramientas de ciberseguridad, segundo trimestre.

No	Herramienta	Fecha de actualización
1	Firmware del equipo FortiSIEM	20/05/2024
2	FortiGate, FortiAnalizer, FortiWeb	21/05/2024

Para el tercer trimestre del año 2024, se efectúan nuevas actualizaciones necesarias para todos los equipos e infraestructura en ciberseguridad que posee el Ministerio de Minas y Energía de tal forma de se tiene la siguiente información:

Tabla 10. Ventanas de mantenimiento a herramientas de ciberseguridad, tercer trimestre.

No	Herramienta	Fecha de actualización
1	Firmware del equipo FortiGate maestro	Tercer trimestre 2024
2	FortiWeb, FortiAnalizer, SIEM, WAF, FW y SandBox	Tercer trimestre 2024

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.

Remitirse al encargado de seguridad de la información a cargo para información detallada de cada evento, resultados y procedimientos.

Ministerio de Minas y Energía

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

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"***

Durante el tercer trimestre, se identificaron una serie de hallazgos clave que forman parte del análisis y generación de actividades dentro del plan de mejora continua en ciberseguridad. Estos hallazgos son fundamentales para reforzar la seguridad de la información en el Ministerio de Minas y Energía. A continuación, se destacan los más relevantes:

Ministerio de Minas y Energía

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

- **Falta de conocimiento en la gestión de incidentes por parte de los usuarios:** A lo largo del año 2024, los incidentes reportados evidenciaron que los usuarios adscritos a la entidad no tenían el conocimiento necesario sobre cómo actuar ante una amenaza o ciberataque. Esto llevó a la creación e implementación de un proceso de gestión de incidentes de seguridad. Este procedimiento, ya descrito en informe, ha sido diseñado para capacitar a los usuarios y establecer un protocolo claro de actuación en caso de incidentes de ciberseguridad.

- **Madurez en ciberseguridad y análisis de amenazas:** Se ha identificado que la entidad se encuentra en un proceso de madurez en ciberseguridad. Como parte de este desarrollo, se hace necesario identificar el perfil de posibles atacantes, sus motivaciones y el impacto que estos pueden generar en la entidad. Por ello, se ha optado por implementar un modelo de identificación de amenazas conocido como **"SOCIA".** Este modelo se ajusta a los fines misionales y estratégicos del Ministerio, considerando que forma parte de la infraestructura crítica de la Nación, y que, por lo tanto, debe cumplir con los lineamientos de ciberdefensa establecidos en diversas normativas nacionales.

- **Actualización de la matriz de activos de información**: Se ha identificado la necesidad urgente de actualizar la matriz de activos de información. Esta herramienta es esencial para determinar la criticidad de los datos que maneja y custodia el Ministerio. Además, servirá como base para otros procesos fundamentales, actualización de un Plan de Recuperación ante Desastres (DRP) y el análisis de Impacto en el Negocio (BIA) por dependencia, garantizando que la protección de los activos más críticos esté alineada con los objetivos de continuidad operativa y resiliencia.

Estos hallazgos y acciones apuntan a fortalecer la postura de ciberseguridad del Ministerio, preparando a la entidad para enfrentar amenazas y garantizar la protección de los activos de información críticos, para saber mayor avance de estos procesos que están en construcción referirse al oficial de seguridad de la información encargado.

PLAN DE SENSIBILIZACIÒN Y CAPACITACIÒN

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.

Ministerio de Minas y Energía

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

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

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.

Ministerio de Minas y Energía

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

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.

1

2

3

4

Ministerio de Minas y Energía

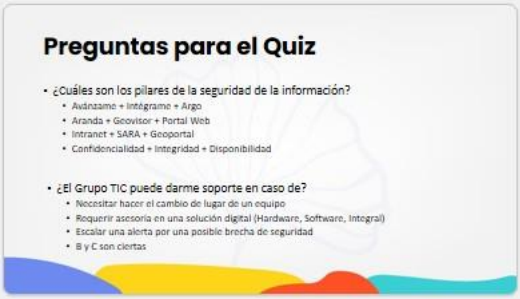
Dirección: Calle 43 No.57 – 31 CAN, Bogotá D.C., Colombia
Conmutador: +57 (601) 220 0300

5

6

7

8



9

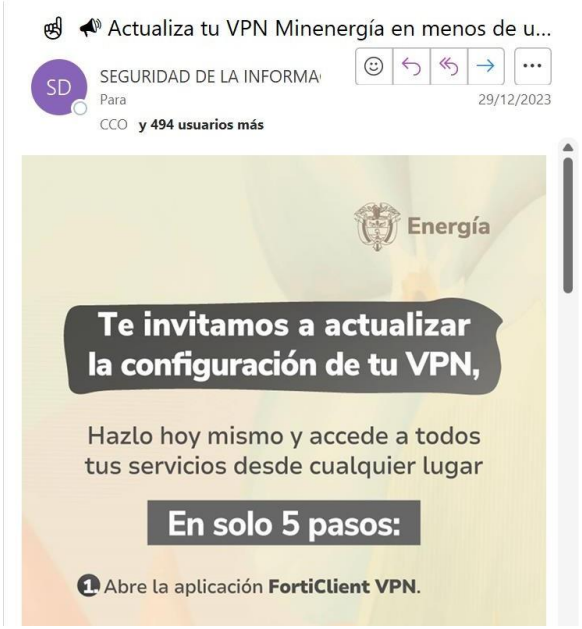
10

• CORREO INSTITUCIONAL

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

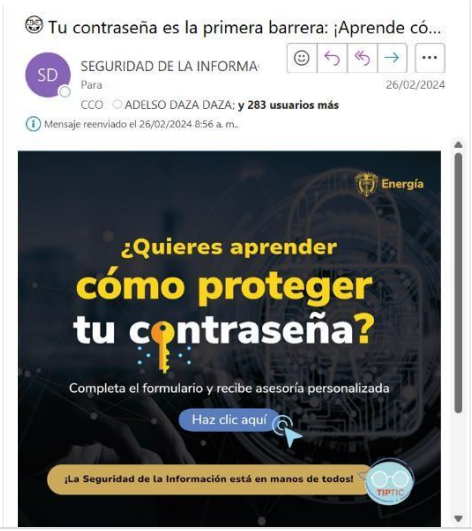
Ministerio de Minas y Energía

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

Correo Electrónico	Detalle de la referencia
	

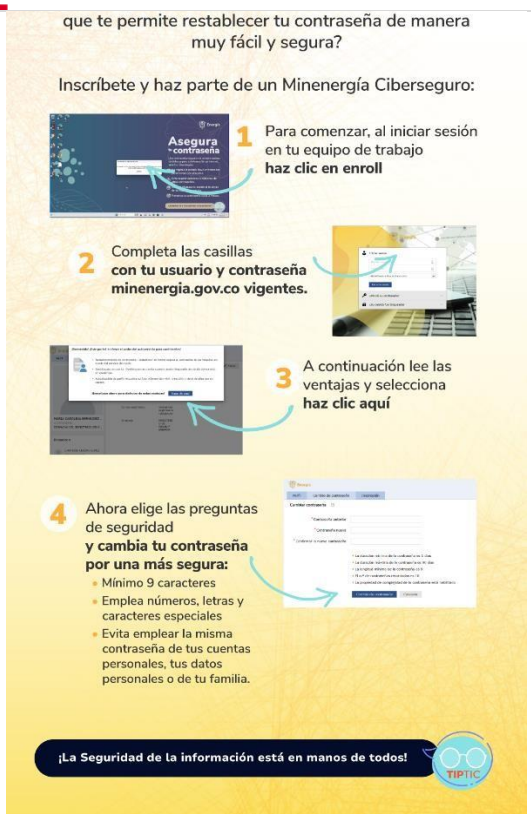
Ministerio de Minas y Energía

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



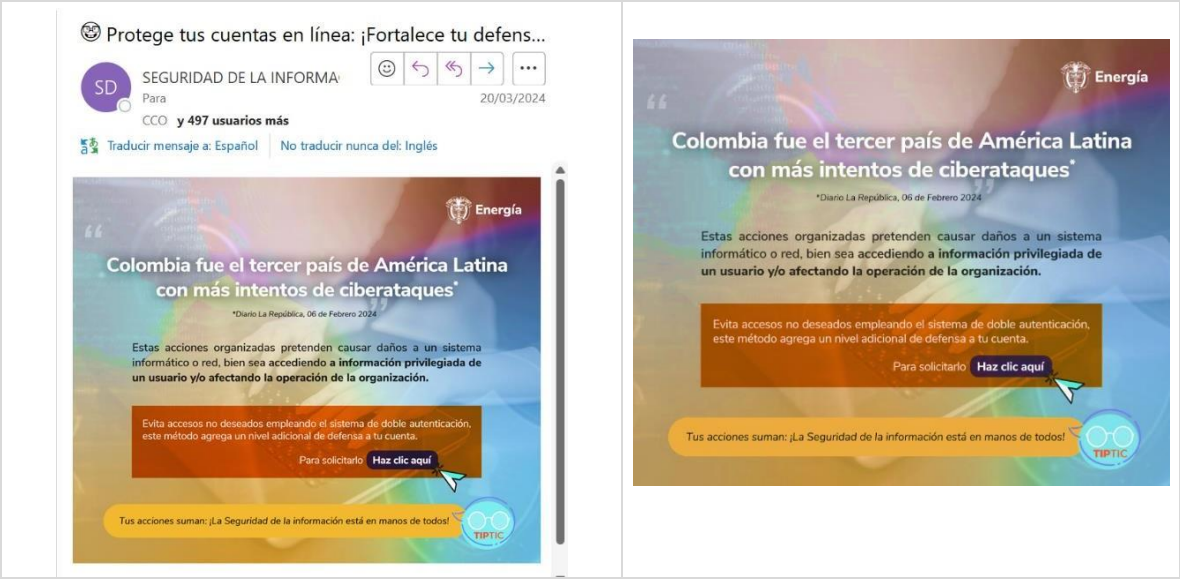
Ministerio de Minas y Energía

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 el contenido publicado 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.

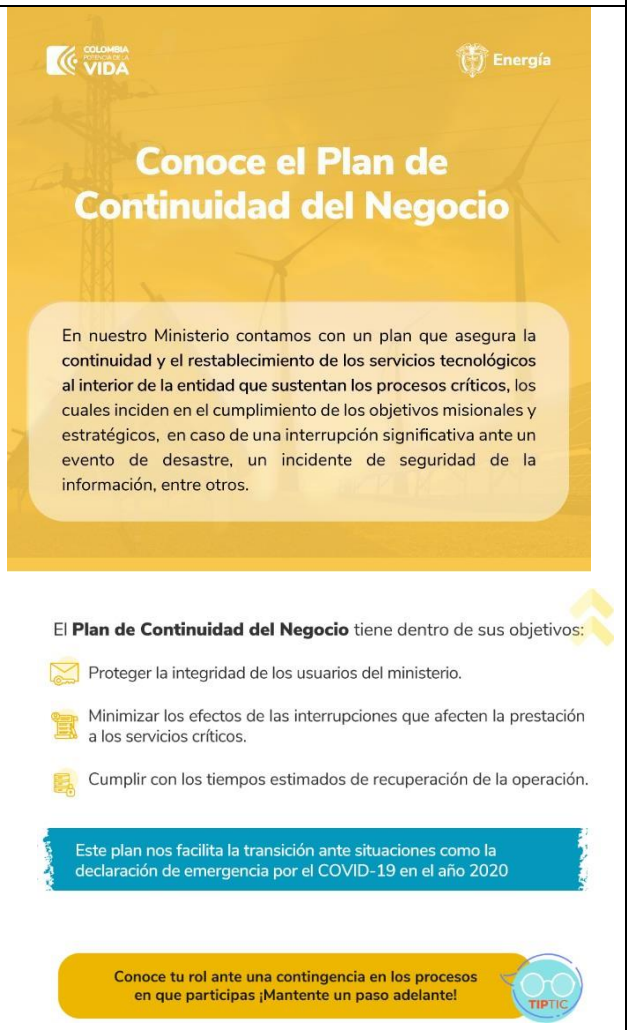
SEGUNDO TRIMESTRE

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.

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.

Ministerio de Minas y Energía

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

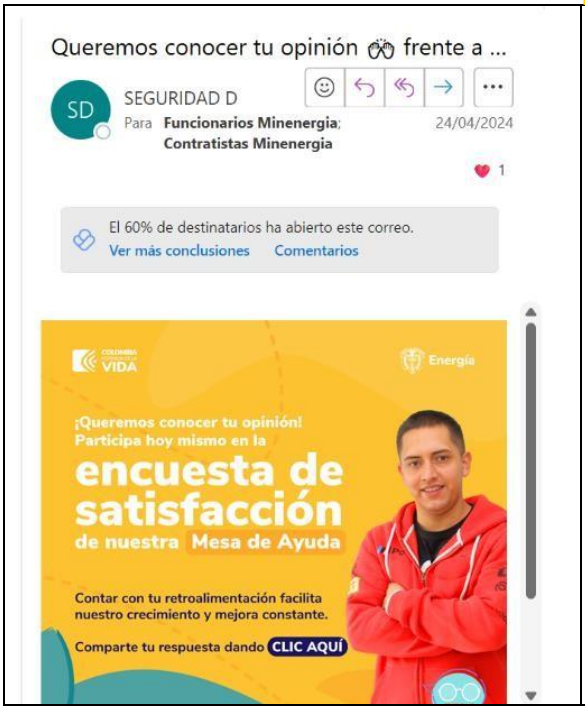
EVIDENCIA DE PUBLICACIÓN	PIEZA
	

Ministerio de Minas y Energía

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

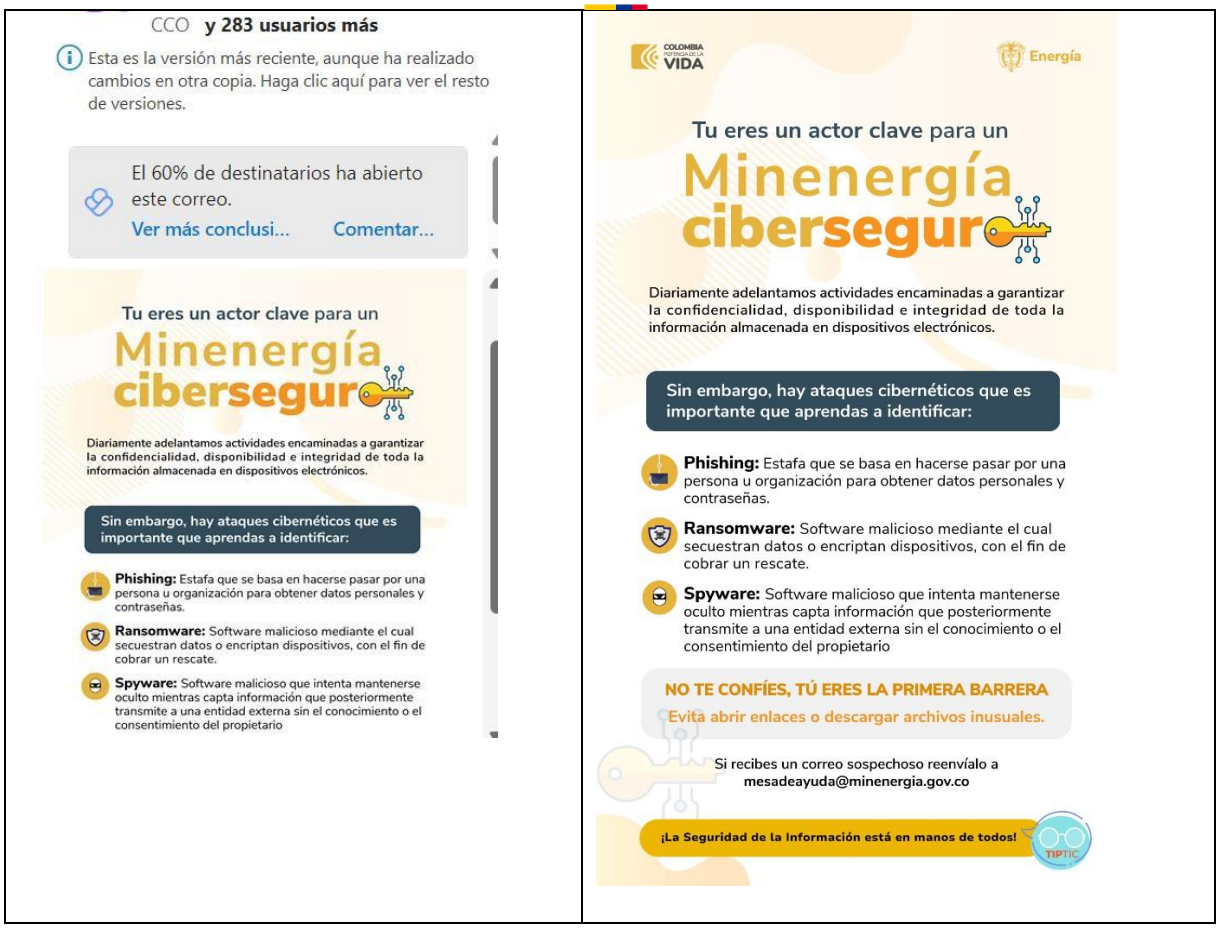
Ministerio de Minas y Energía

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



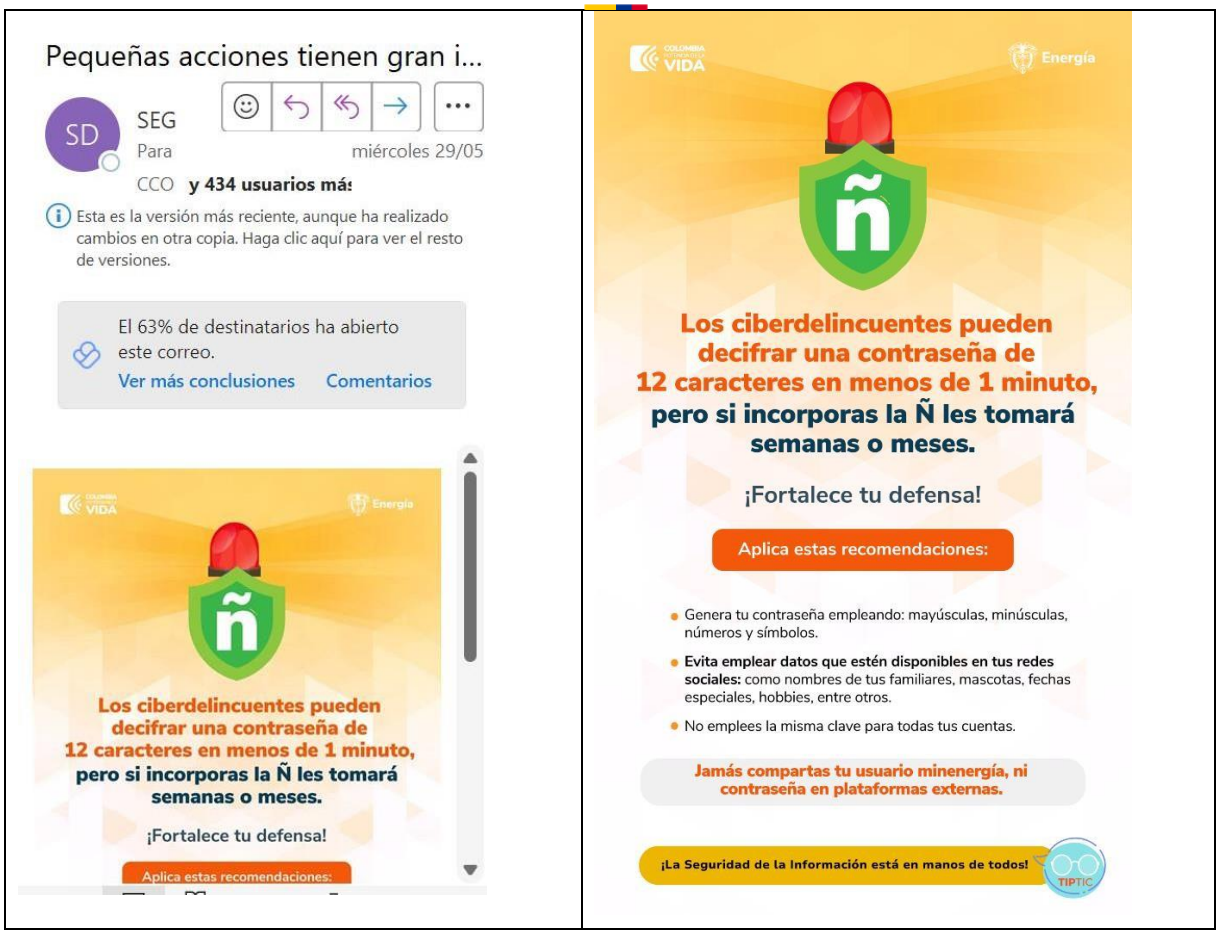
Ministerio de Minas y Energía

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



Ministerio de Minas y Energía

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



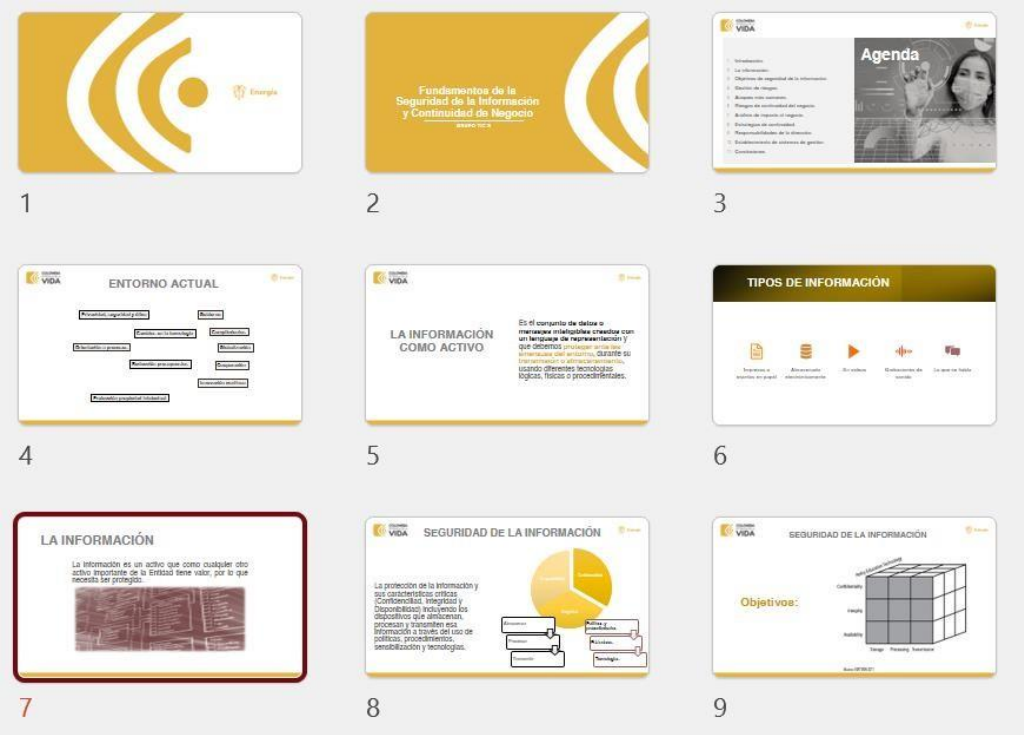
Continuaremos revisando constantemente los contenidos de este programa y su desempeño en lectura, para adherir las buenas prácticas entre los usuarios y usar las herramientas TIC.

Ministerio de Minas y Energía

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

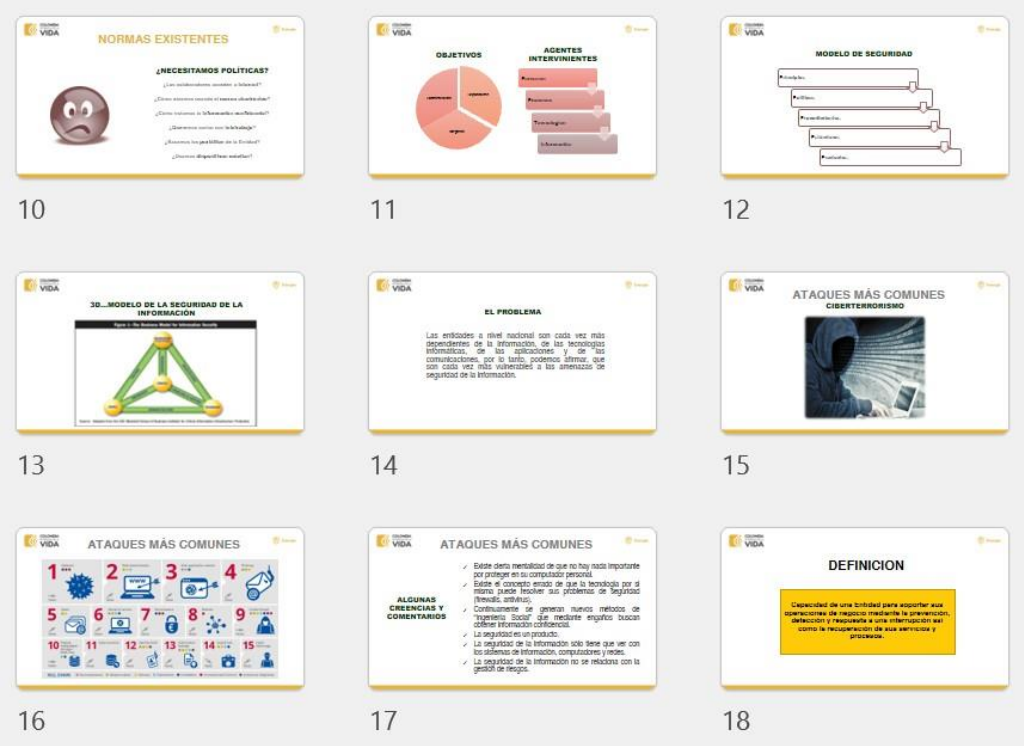
6.1 Capacitación

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

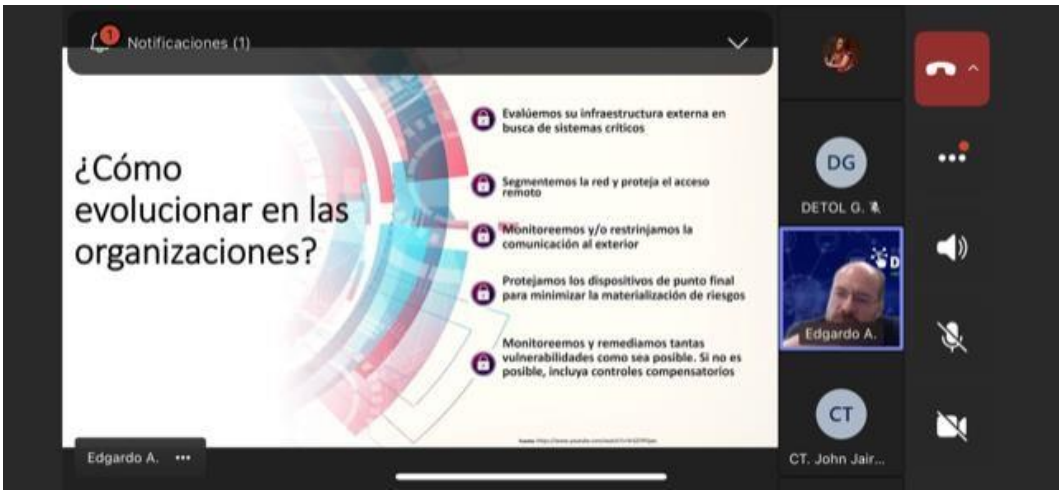


Ministerio de Minas y Energía

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



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:



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 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 MME.

Para el tercer trimestre, se ha establecido el siguiente cronograma de capacitaciones, en línea con lo descrito en el trimestre anterior. Las temáticas seleccionadas responden a las necesidades actuales del Ministerio y han sido diseñadas teniendo en cuenta la evolución de las amenazas emergentes en el ciberespacio. Este enfoque asegura que los funcionarios y contratistas estén preparados para enfrentar los desafíos más recientes en materia de ciberseguridad y protección de la información.

Tabla 11. Cronograma de capacitaciones de seguridad de la información.

Fecha	Tema	Título Atractivo	Descripción
21-oct	Fundamentos de Seguridad de la información, ciberseguridad y principales amenazas - PARTE 1	"Blindando la Energía Digital: Defiéndete de las Amenazas Cibernéticas ¿Información?"	Conceptos básicos de seguridad de la información, importancia de la protección de datos, principios de confidencialidad, integridad y disponibilidad.
30-oct	Fundamentos de Seguridad de la información, ciberseguridad y principales amenazas - PARTE 2		Descripción de las principales amenazas cibernéticas (malware, phishing, ransomware), cómo reconocerlas y protegerse de ellas.
Noviembre - semana por definir	Políticas de Seguridad y Privacidad del Ministerio	"Energizando la Seguridad: Conoce las Políticas del MINENERGIA"	Explicación detallada de las políticas de seguridad de la información y privacidad que el ministerio ha implementado, y cómo cumplirlas en el día a día.

Ministerio de Minas y Energía

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

Noviembre - semana por definir	Gestión de Incidentes de Seguridad	"¡Actúa como un Generador de Seguridad! Gestión Eficaz de Incidentes"	Cómo responder a un incidente de seguridad, protocolo de acción ante amenazas, y reporte de incidentes. Taller práctico de simulación de incidentes.
Diciembre - semana por definir	Plan de Recuperación ante Desastres (DRP) y Continuidad de Negocio	"Resiliencia Energética: Plan de Recuperación y Continuidad del MINENERGIA"	Explicación del DRP del ministerio, la importancia de la continuidad operativa y cómo reaccionar ante eventos que comprometan los sistemas.
Diciembre - semana por definir	Política de tratamiento de datos personales	"Ciberseguridad: Mantén Encendida la Llama de la Protección Digital"	Reforzamiento de la cultura de ciberseguridad a través de la concientización de las mejores prácticas, con ejemplos de la vida diaria y cómo aplicarlas en el trabajo, alineados a la política de tratamiento de datos personales.

En conclusión, el cronograma de capacitaciones para el tercer trimestre se ha diseñado estratégicamente para fortalecer la cultura de ciberseguridad en el Ministerio de Minas y Energía. Las temáticas propuestas abordan de manera integral las necesidades de la entidad, enfocándose en los fundamentos de seguridad de la información, la gestión de incidentes, y las políticas de privacidad y recuperación ante desastres. Al ajustar los contenidos a las amenazas emergentes en el ciberespacio, se garantiza que los funcionarios y contratistas estarán mejor preparados para proteger los activos críticos del Ministerio y mitigar riesgos potenciales.

Este esfuerzo, alineado con los lineamientos estratégicos del Ministerio, busca consolidar un entorno seguro y resiliente, capaz de responder a los crecientes desafíos del entorno digital. La continuidad de estas capacitaciones y la adopción de mejores prácticas asegurarán que el Ministerio de Minas y Energía siga liderando el camino hacia una ciberdefensa sólida, manteniendo protegidos sus sistemas y procesos esenciales ante posibles ciberataques.

Ministerio de Minas y Energía

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

Energía