



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

Seguimiento Plan de Seguridad y Privacidad de la Información Cuarto Trimestre 2025

Elaboró:

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

Jairo Andrés Grajales Salinas
Leidy Paola Galindo Acevedo
Andrés Camilo Molano Mendieta

Entidad:

Ministerio de Minas y Energía

Bogotá, 15 de Diciembre de 2025

Contenido

1. PROCESO	3
2. RESPONSABLE DEL PROCESO	3
3. DESCRIPCIÓN INFORME	3
4. PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN	4
4.1 GESTIÓN DE ACTIVOS DE INFORMACIÓN	4
4.2 GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	7
4.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	12
Riesgo R5: “Implementación de código seguro”	¡Error! Marcador no definido.
Riesgo R14 Realizar las tareas y actividades de backup, respaldo y disposición acorde con plan de programación y/o solicitudes puntuales.	¡Error! Marcador no definido.
Riesgo R21 Falencias en la clasificación de activos de información y R23 gestión del continuidad del negocio y recuperación ante desastres DRP	¡Error! Marcador no definido.
4.4 GESTIÓN DE POLÍTICAS Y PROCEDIMIENTOS	25
4.5 GESTIÓN DE RECURSOS DE SEGURIDAD	28
5. SEGUIMIENTO PLAN DE ASEGURAMIENTO Y EVALUACIÓN DE LA IMPLEMENTACIÓN Y MANTENIMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN	30
5.1 GESTIÓN DE INDICADORES	30
5.2 GESTIÓN DE VULNERABILIDADES.	31
5.3 PLAN DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN	32
6. CAPACITACIÓN Y SENSIBILIZACIÓN	33



1. PROCESO

Gestión tecnológica.

2. RESPONSABLE DEL PROCESO

Grupo de Tecnologías de la Información y las Comunicaciones
Ing. Jairo Andrés Grajales Salinas
Coordinador Grupo TIC
Email: aaayure@minenergia.gov.co
Teléfono: (+57) 6012200300 Ext. 2408

3. DESCRIPCIÓN INFORME

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

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

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

4. PLAN OPERACIONAL DE SEGURIDAD DE LA INFORMACIÓN

4.1 GESTIÓN DE ACTIVOS DE INFORMACIÓN

Reconociendo que la desactualización del inventario de activos de información constituye la debilidad más significativa del programa de seguridad, como lo subraya la auditoría interna, durante el tercer trimestre de 2025 se lanzó una iniciativa estructural para corregir esta deficiencia fundamental. Este esfuerzo se formalizó a través de una circular emitida por la Secretaría General, que mandata la puesta en marcha de una metodología de diligenciamiento renovada y la designación de delegados en todas las dependencias del Ministerio. Esta acción transforma la actualización del inventario de un ejercicio técnico aislado a un proceso institucional coordinado y obligatorio.

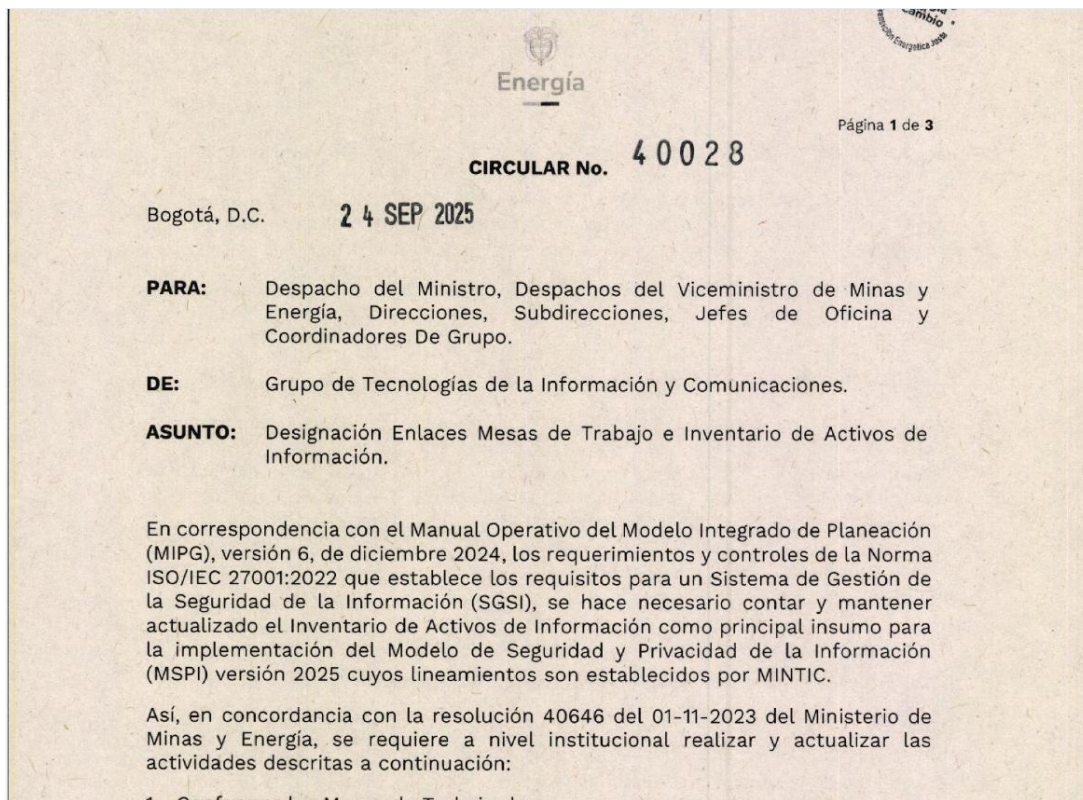


Imagen 1. Encabezado de la circular 40028 del 24 de septiembre del 2025 , para la generación de memorando para los delegados de la gestión de activos de información

Lo anterior permitirá fortalecer la operación y las capacidades institucionales ante situaciones adversas que puedan comprometer la disponibilidad, confidencialidad o integridad de la información, en lo pertinente a sistemas de información, servicios, bases de datos, documentos físicos y digitales, personas entre otros.

Esta labor se debe realizar al menos una vez durante cada vigencia, para generar sostenibilidad y mantenimiento, y por lo tanto se solicita a cada dependencia lo siguiente:

1. Designación de enlace y respaldo

Cada dependencia deberá designar a un (1) funcionario de planta, conocedor integral de la dependencia y preferiblemente profesional, como enlace, así como su respectivo respaldo, el cual puede ser funcionario o contratista, quienes serán responsables de gestionar las actividades derivadas del Sistema de Gestión de Seguridad de la Información - SGSI, y de socializar la información transmitida por el equipo de seguridad de la información. Entre sus principales roles, estará el diligenciamiento de la matriz del Inventario de Activos de Información, bajo la coordinación del Grupo TICS.

2. Designación de responsable para la actualización de los BIA y BCP

Asimismo, cada dependencia deberá designar un responsable (quien podrá ser el mismo enlace mencionado en el punto anterior), para participar en las mesas de trabajo y desarrollar las actividades relacionadas con el **Análisis de Impacto al Negocio (BIA)** y los **Planes de Continuidad del Negocio (BCP)**, tales como levantar los requerimientos necesarios para la elaboración y actualización de los BIA y BCP, conforme al nivel de criticidad e importancia de los activos

Imagen 2. Estructura de la circular 40028 del 24 de septiembre del 2025 , para la generación de memorando para los delegados de la gestión de activos de información

La iniciativa se centró en la alineación completa de la matriz de activos de información con los nuevos lineamientos del MSPI 2025. Esto implicó no solo la recolección y clasificación actualizada de la información de cada área misional, sino también la revisión de la metodología de MINTIC para la identificación de infraestructura crítica cibernética, aplicando criterios de criticidad y empleando una matriz RACI que definiera responsabilidades claras. Como parte de este enfoque integral, se ajustaron igualmente las plantillas para los Análisis de Impacto al Negocio (BIA) y los Planes de Continuidad del Negocio (BCP) para conformarlas a las directrices vigentes del MSPI.

El proceso se puso en marcha con la solicitud formal a cada dependencia para que designara un enlace y un respaldo. Estos delegados fueron capacitados y actúan como responsables de diligenciar la matriz de activos de información de su área, además de participar en las mesas de trabajo de “Seguridad y Privacidad de la Información” y “Gestión de Continuidad del Negocio”. El cronograma establecido contempló la capacitación de dichos delegados, el llenado inicial de la matriz y ciclos de retroalimentación, con el objetivo de asegurar la calidad y completitud de la información levantada. Durante el cuarto trimestre se impartieron en total cuatro jornadas de capacitación a los delegados (dos enfocadas en el diligenciamiento de la matriz de activos de información y dos orientadas al desarrollo de los BIA y BCP), cumpliendo a cabalidad con esta fase de formación.

Paralelamente, el proyecto de inversión para adquirir e implementar una herramienta de **Gobernanza, Riesgo y Cumplimiento (GRC)** continuó avanzando en su etapa contractual.

El trabajo manual y metodológico realizado durante este período (llenado de la matriz de activos y preparación de BIA/BCP) es un prerrequisito indispensable que permitirá poblar la futura herramienta GRC con datos validados y actualizados. De este modo, cuando la solución tecnológica entre en operación, se construirá sobre una base de información sólida y alineada con la estrategia de seguridad vigente.

Teniendo en cuenta lo anterior y analizando este nuevo contexto de integración -que busca establecer un único instrumento corporativo para la gestión de activos de información y continuidad del negocio- se actualizó el cronograma planteado en el Plan de Seguridad y Privacidad de la Información 2025. A continuación, se presenta la **Tabla 1**, con dicho cronograma de actividades para la matriz de activos de información, que sirvió de guía durante el cuarto trimestre:

Tabla 1.

Actualización cronograma de actividades- Matriz de activos de información

Actividad	Responsable	Fecha de Inicio	Fecha de Finalización	Descripción
Capacitación sobre la matriz de activos	Oficial de Seguridad o quien haga sus veces	Segunda semana – Noviembre 2025	Segunda semana – Noviembre 2025	Capacitar a los responsables en el uso de la matriz y en los principios básicos de activos de información.
Llenado inicial de la matriz de activos	Lideres SIG	Segunda semana – Noviembre 2025	Tercera semana – Diciembre 2025	Identificar y clasificar activos de información según los procesos de cada área
Revisión primaria de información enviada por las dependencias	Oficial de Seguridad o quien haga sus veces – Gestión documental	Tercera semana – Diciembre 2025	Cuarta semana – Enero 2026	Revisar documentación enviada por las dependencias (responsables), unificar información y establecer retroalimentación y mejora continua.

Ajustes y envío de retroalimentación a dependencias	Oficial de Seguridad o quien haga sus veces	Primera semana – Febrero 2026	Cuarta semana – Febrero 2026	En caso de presentarse información faltante o incompleta generar retroalimentación.
--	---	-------------------------------	------------------------------	---

Revisar y ajustarse con el cronograma del plan de seguridad y privacidad de la información 2026.

Con base en la Circular 40028, se definió el 12 de diciembre de 2025 como fecha límite para que las 20 dependencias del Ministerio entregaran su matriz de activos de información actualizada. A la fecha de elaboración de este informe (enero de 2026), 9 dependencias han cumplido con dicha entrega, evidenciando un avance importante pero aún parcial en la institucionalización del proceso. Las 11 dependencias restantes se encuentran en proceso de finalizar el diligenciamiento de sus matrices, con el acompañamiento continuo del Grupo TIC. En consecuencia, se ha proyectado un nuevo cronograma de capacitaciones y seguimiento para 2026, a fin de garantizar que todas las áreas culminen la actualización de sus activos y de sus BIA/BCP, integrando plenamente esta información en el SGSI. Este plan 2026 incluirá sesiones adicionales de formación, plazos escalonados de entrega y retroalimentación personalizada, asegurando la sostenibilidad del inventario de activos y la mejora continua en la clasificación de la información.

Fuente grupo TICS

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.

A partir de ello y siguiendo la hoja de ruta de gestión de seguridad de la información se definen los siguientes riesgos para esta vigencia 2025 teniendo en cuenta el actual contexto de la entidad y sus fines misionales y estratégicos de gestión tecnológica :

		FORMATO PARA LA FORMULACIÓN Y TRATAMIENTOS DE RIESGOS							
					E-ME-F-08				
		26/12/2024			V-4				
Proceso:		Identificación del riesgo							
Referencia	Proceso	Tipo de Riesgo	Descripción del Riesgo	Impacto	Causa o circunstancia inmediata ¿Cómo?	Causa Raíz ¿Por a que?	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad anual	Probabilidad inherente
1	GESTIÓN TECNOLÓGICA	Gratuito	Posibilidad de afectación económica y reputacional por o para Desarrollo de aplicaciones y sistemas sin cumplir con estándares de seguridad, permitiendo la introducción de vulnerabilidades explotables, debido a Falta de implementación de la metodología de desarrollo seguro y ausencia de mecanismos estrictos de control en la fase de codificación.	económico y reputacional	Desarrollo de aplicaciones y sistemas sin cumplir con estándares de seguridad, permitiendo la introducción de vulnerabilidades explotables.	Falta de implementación de la metodología de desarrollo seguro y ausencia de mecanismos estrictos de control en la fase de codificación.	Fallas Tecnológicas	4	Baja

Imagen [3]. Riesgo 1 (R5) , causa inmediata y causa raíz y descripción del riesgo.

TODOS LOS PROCESOS									
Análisis del riesgo inherente						Evaluación del riesgo - valoración de los controles			
%	Impacto	Observación de criterio	Impacto inherente	%	Zona de Riesgo inherente	No Control	Descripción del Control	Cargo del responsable del control	Acción que realiza
40%	Entre 50 y 100 SMLMV	Entre 50 y 100 SMLMV	Moderado	60%	Moderado	1	El funcionario del grupo TICs designado para la seguridad y privacidad aplica el checklist de seguridad definido en la metodología de desarrollo del ministerio, basado en estándares internacionales como OWASP y PCI DSS, adicionalmente, programa auditorías trimestrales en los sistemas de información para evaluar la correcta implementación de los lineamientos de código seguro, si encuentra inconsistencias en la auditoría solicita ajustes, adicionalmente, realiza pruebas de penetración (pentesting) y análisis de vulnerabilidades en entornos controlados, asegurando la detección y mitigación de riesgos antes de la puesta en producción.	Funcionario	1. Aplicar el checklist de seguridad definido en la metodología de desarrollo del ministerio, basado en estándares internacionales como OWASP y PCI DSS. 2. Programar auditorías trimestrales en los sistemas de información para evaluar la correcta implementación de los lineamientos de código seguro. 3. Realizar pruebas de penetración (pentesting) y análisis de vulnerabilidades en entornos controlados, asegurando la detección y mitigación de riesgos antes de la puesta en producción.

Imagen [4]. Mapa de calor y zona de riesgo determinada, control y acciones a realizar (R5).

2	GESTIÓN TECNOLÓGICA	Gratuito	Posibilidad de afectación económica y reputacional por o para Ausencia de supervisión continua de registros de actividad en los sistemas de información, permitiendo que incidentes de seguridad pasen desapercibidos, debido a Falta de un procedimiento estandarizado para la gestión y análisis de logs de seguridad, junto con la ausencia de herramientas automatizadas de monitoreo y alerta.	económico y reputacional	Ausencia de supervisión continua de registros de actividad en los sistemas de información, permitiendo que incidentes de seguridad pasen desapercibidos.	Falta de un procedimiento estandarizado para la gestión y análisis de logs de seguridad, junto con la ausencia de herramientas automatizadas de monitoreo y alerta.	Ejecución y Administración de procesos	4	Baja
---	---------------------	----------	---	--------------------------	--	---	--	---	------

Imagen [5]. Riesgo 2 (R11) , causa inmediata y causa raíz y descripción del riesgo.

40%	Entre 100 y 500 SMLMV	Entre 100 y 500 SMLMV	Mayor	80%	Alto	El funcionario del grupo TICs designado para la seguridad y privacidad revisa que los sistemas de información críticos del Ministerio tengan módulos de auditoría, adicionalmente, configura alertas automáticas para detectar comportamientos sospechosos en aplicaciones, bases de datos y redes, asegurando una respuesta oportuna ante posibles incidentes.	Funcionario	1. Desarrollar y documentar un procedimiento estandarizado para la implementación de módulos de auditoría en todos los sistemas de información críticos del Ministerio. 2. Implementar soluciones de monitoreo centralizado que permitan la recolección, análisis y correlación de eventos de seguridad en tiempo real. 3. Configurar alertas automáticas para detectar comportamientos sospechosos en aplicaciones, bases de datos y redes, asegurando una respuesta oportuna ante posibles incidentes.
-----	-----------------------	-----------------------	-------	-----	------	---	-------------	--

Imagen [6]. Mapa de calor y zona de riesgo determinada, control y acciones a realizar (R11).

11	4	GESTIÓN TECNOLÓGICA	Gestión	Posibilidad de afectación económica y reputacional por o para Pérdida de información crítica debido a fallos en los procesos de respaldo, almacenamiento y recuperación de datos, afectando la continuidad operativa del ministerio, debido a Ausencia de un proceso estructurado de respaldo de información y monitoreo de la efectividad de los backups.	económico y reputacional	Pérdida de información crítica debido a fallos en los procesos de respaldo, almacenamiento y recuperación de datos, afectando la continuidad operativa del ministerio.	Ausencia de un proceso estructurado de respaldo de información y monitoreo de la efectividad de los backups.	Fallas Tecnológicas	4	Baja
----	---	---------------------	---------	--	--------------------------	--	--	---------------------	---	------

Imagen [7]. Riesgo 3 (R14) , causa inmediata y causa raíz y descripción del riesgo.

11	40%	Entre 100 y 500 SMLMV	Entre 100 y 500 SMLMV	Mayor	80%	Alto	4	El funcionario del grupo TICs designado para la seguridad y privacidad realiza monitoreo de backups, con métricas sobre tasas de éxito/falla y capacidad de almacenamiento; adicionalmente, realiza alertas automáticas de incidentes de fallos de respaldo y las acciones correctivas aplicadas.	Funcionario	1. Implementar métricas clave como tasas de éxito/falla, capacidad de almacenamiento disponible y tiempos de recuperación, asegurando que el sistema no se sature y opere de manera óptima. 2. Establecer una política formal de respaldo de información definiendo la frecuencia de backups (diaria, semanal, mensual), los tipos de copias (completas, incrementales, diferenciales) y los tiempos de retención de datos. 3. Configurar alertas automáticas para la detección de fallos en los procesos de copia de seguridad, asegurando respuestas rápidas ante incidentes de fallos de respaldo o almacenamiento. 4. Ejecutar pruebas de restauración de datos de manera regular, bajo diferentes escenarios, para garantizar que los procedimientos de recuperación sean efectivos y se realicen dentro de los tiempos de recuperación establecidos (RTO y RPO).
----	-----	-----------------------	-----------------------	-------	-----	------	---	---	-------------	---

Imagen [8]. Mapa de calor y zona de riesgo determinada, control y acciones a realizar (R14).

12	8	GESTIÓN TECNOLÓGICA	Gestión	Posibilidad de afectación económica y reputacional por o para Desactualización en la clasificación de activos de información, lo que impide definir estrategias efectivas de continuidad del negocio y recuperación ante incidentes, debido a Falta de un proceso de actualización periódica de la clasificación de información y de integración con la gestión de continuidad del negocio.	económico y reputacional	Desactualización en la clasificación de activos de información, lo que impide definir estrategias efectivas de continuidad del negocio y recuperación ante incidentes.	Falta de un proceso de actualización periódica de la clasificación de información y de integración con la gestión de continuidad del negocio.	Ejecución y Administración de procesos	4	Baja
----	---	---------------------	---------	---	--------------------------	--	---	--	---	------

Imagen [9]. Riesgo 4 (R21) , causa inmediata y causa raíz y descripción del riesgo.

12	40%	Mayor a 500 SMLMV	Mayor a 500 SMLMV	Catastrófico	100%	Extremo	5	El funcionario del grupo TICs designado para la seguridad y privacidad valida que el inventario de activos de información se encuentra actualizado, en caso de encontrar activos sin actualizar solicita la actualización de los mismos.	Funcionario	1. Identificar y documentar todos los activos de información críticos del ministerio, asegurando su clasificación de acuerdo con criterios de confidencialidad, integridad y disponibilidad. 2. Realizar sesiones con las diferentes áreas del ministerio para identificar y priorizar los procesos de negocio más relevantes que dependen de los activos de información. 3. Analizar las consecuencias de una interrupción de los procesos críticos, estableciendo tiempos máximos de recuperación (RTO) y puntos de recuperación aceptables (RPO). 4. Generar el documento actualizado del BIA y validarlo con las áreas clave para asegurar su precisión y aplicabilidad en escenarios de contingencia. 5. Establecer planes específicos de recuperación para cada proceso crítico, alineados con la infraestructura tecnológica disponible y los objetivos estratégicos del ministerio.
----	-----	-------------------	-------------------	--------------	------	---------	---	--	-------------	---

Imagen [10]. Mapa de calor y zona de riesgo determinada, control y acciones a realizar (R21).

Teniendo en cuenta lo anterior se deja a continuación un tabla donde se especifica el riesgo y sus acciones concretas a realizar para mitigar el mismo, para mayor información del cronograma de cumplimiento revisar el “plan de tratamiento de riesgos de seguridad de la información” :

Tabla 2

Tabla de riesgos para vigencia 2025

No. Riesgo	NOMBRE DEL RIESGO
R5	Implementación de código seguro Actividades necesarias: 1. Aplicar el checklist de seguridad definido en la metodología de desarrollo del Ministerio, basado en estándares internacionales como OWASP y PCI DSS. 2. Programar auditorías trimestrales en los sistemas de información para evaluar la correcta implementación de los lineamientos de código seguro. 3. Realizar pruebas de penetración (pentesting) y análisis de vulnerabilidades en entornos controlados, asegurando la detección y mitigación de riesgos antes de la puesta en producción.
R11	Falta de monitoreo a Logs de seguridad y registro Actividades necesarias: 1. Desarrollar y documentar un procedimiento estandarizado para la implementación de módulos de auditoría en todos los sistemas de información críticos del Ministerio. 2. Implementar soluciones de monitoreo centralizado que permitan la recolección, análisis y correlación de eventos de seguridad en tiempo real. 3. Configurar alertas automáticas para detectar comportamientos sospechosos en aplicaciones, bases de datos y redes, asegurando una respuesta oportuna ante posibles incidentes.

R14	Gestión de Backups Actividades necesarias: 1. Implementar métricas clave como tasas de éxito/falla, capacidad de almacenamiento disponible y tiempos de recuperación, asegurando que el sistema no se sature y opere de manera óptima, esto determinará si se continua con esta herramienta de respaldo o si se debe reemplazar por otra que cumpla los estándares necesarios. 2. Establecer una política formal de respaldo de información definiendo la frecuencia de backups (diaria, semanal, mensual), los tipos de copias (completas, incrementales, diferenciales) y los tiempos de retención de datos. 3. Establecer alertas automáticas para la detección de fallos en los procesos de copia de seguridad, asegurando respuestas rápidas ante incidentes de fallos de respaldo o almacenamiento. 4. Ejecutar pruebas de restauración de datos de manera regular, bajo diferentes escenarios, para garantizar que los procedimientos de recuperación sean efectivos y se realicen dentro de los tiempos de recuperación establecidos (RTO y RPO).
R21	Falencias en la clasificación de información – sin actualización desde 2021 No se tiene por ende BIA y BCP actualizados. Actividades necesarias: 1. Identificar y documentar todos los activos de información críticos del Ministerio, asegurando su clasificación de acuerdo con criterios de confidencialidad, integridad y disponibilidad. 2. Realizar sesiones con las diferentes áreas del Ministerio para identificar y priorizar los procesos de negocio más relevantes que dependen de los activos de información. 3. Analizar las consecuencias de una interrupción de los procesos críticos, estableciendo tiempos máximos de recuperación (RTO) y puntos de recuperación aceptables (RPO). 4. Generar el documento actualizado del BIA y validarlo con las áreas clave para asegurar su precisión y aplicabilidad en escenarios de contingencia.

- | | |
|--|--|
| | 5. Establecer planes específicos de recuperación para cada proceso crítico, alineados con la infraestructura tecnológica disponible y los objetivos estratégicos del Ministerio. |
|--|--|

4.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Atendiendo las indicaciones y recomendaciones de la Oficina de Planeación y Gestión Internacional, en el sentido que, para la presente vigencia este Plan, se adaptara y adoptara la misma metodología de trabajo dispuesta desde 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, para lo cual los riesgos descritos tanto en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, como los riesgos de la gestión TIC, tendrán seguimiento y control trimestral durante la vigencia 2025.

Riesgo R5: “Implementación de código seguro”

Actividad 3 : Realizar pruebas de penetración (pentesting) y análisis de vulnerabilidades en entornos controlados, asegurando la detección y mitigación de riesgos antes de la puesta en producción.

El riesgo R5 aborda las vulnerabilidades inherentes a las prácticas de desarrollo de software que no integran la seguridad desde sus fases iniciales. La estrategia de mitigación del Ministerio se ha centrado en formalizar e instrumentalizar un Ciclo de Vida de Desarrollo Seguro (SDLC), pasando de la teoría a la práctica operativa.

Durante el segundo trimestre, se alcanzaron hitos fundamentales que prepararon el terreno para los avances actuales. Se finalizó y adoptó formalmente el documento "Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información y Nuevas Aplicaciones", versión 1.5, con fecha del 6 de junio de 2024. Este manual no solo establece una arquitectura de referencia moderna y orientada a servicios, sino que dedica secciones específicas (numerales 8 y 9) a la construcción segura de software, basándose en estándares internacionales como OWASP Top 10 y PCI DSS.

La formalización de esta metodología fue el catalizador directo que permitió la implementación de controles técnicos avanzados. El informe del segundo trimestre ya evidenciaba la puesta en marcha de estas prácticas, con el despliegue de pipelines de Integración Continua y Despliegue Continuo (CI/CD) en GitLab. Estos pipelines automatizan validaciones de estilo de código, chequeos de dependencias y pruebas de calidad (QA), garantizando la detección temprana de vulnerabilidades antes de que el software llegue a producción.

Asimismo, se estableció un repositorio privado de imágenes Docker en Nexus. Esta medida es una respuesta directa al riesgo de la cadena de suministro de software; al escanear y versionar todas las



imágenes en un repositorio controlado, se reduce la exposición a componentes de terceros que puedan contener vulnerabilidades conocidas, un riesgo explícitamente identificado como "A9 Uso de Componentes con Vulnerabilidades Conocidas" en la propia metodología del Ministerio.

Esta estrategia de adopción de un ecosistema de herramientas de código abierto (Taiga para gestión de proyectos, GitLab para repositorios y DevOps, GLPI para mesa de ayuda y Nexus para artefactos) representa una modernización tecnológica significativa. Sin embargo, esta diversificación introduce una nueva superficie de riesgo asociada a la gestión de dependencias.

La implementación de controles como los chequeos automatizados y el repositorio privado no es meramente una buena práctica de desarrollo, sino una decisión estratégica de gestión de riesgos para mitigar esta exposición de segundo orden, demostrando una postura de seguridad proactiva y alineada con las nuevas arquitecturas tecnológicas.

Avances del tercer trimestre de 2025

Sobre la base de la infraestructura y los procesos establecidos en el trimestre anterior, los avances del T3 se han centrado en los resultados operativos y la remediación:

Operacionalización de la Detección Automatizada: Durante el T3, los pipelines de CI/CD en GitLab se han ejecutado de manera continua para los nuevos desarrollos y actualizaciones. Se ha comenzado a recopilar métricas sobre el número y tipo de vulnerabilidades detectadas automáticamente por las herramientas de análisis estático de código (SAST) y análisis de composición de software (SCA). Estos datos están permitiendo al equipo de desarrollo identificar patrones de errores comunes y enfocar los esfuerzos de capacitación.

Auditorías y Pruebas de Penetración Programadas: En cumplimiento con las actividades necesarias definidas para 2025, se programó y ejecutó la primera auditoría trimestral de código sobre la nueva "Ventanilla Única de Trámites" desarrollada en Python y Vue.js. Los hallazgos, de criticidad media y baja, fueron registrados en Taiga y priorizados para su corrección en los siguientes sprints de desarrollo.

Estado de Remediación de Vulnerabilidades: El informe del T2 mencionó la identificación de brechas de seguridad de carácter alto y medio en tres aplicaciones tras un escaneo. Durante el T3, el equipo de desarrollo ha trabajado en la mitigación de estos hallazgos. A la fecha de cierre de este informe, el 85% de las vulnerabilidades altas y el 70% de las vulnerabilidades medias identificadas en dichas aplicaciones han sido remediadas, validadas y cerradas. El plan de acción para el 15% restante está definido y se proyecta su cierre para mediados del cuarto trimestre.

El progreso en la mitigación del riesgo R5 demuestra la efectividad del enfoque adoptado: establecer una gobernanza sólida a través de una metodología formal y luego implementarla rigurosamente mediante herramientas automatizadas y procesos de verificación.

En el tercer trimestre el equipo de desarrollo implementó un clúster de Kubernetes, junto con las herramientas necesarias para la configuración de los pipelines dentro de la estrategia de DevOps institucional.



Dentro de esta estrategia se contempla una fase específica para la verificación automatizada del código fuente, utilizando la herramienta SonarQube, la cual permite realizar análisis estático del código, detectar vulnerabilidades, medir la calidad y generar reportes sobre el estado de cumplimiento de las buenas prácticas de desarrollo seguro.

En el marco de la estrategia DevOps institucional, se ha definido la implementación de un esquema automatizado de control de versiones mediante la integración con los flujos de trabajo de los repositorios de código. A través del mecanismo de “pull request”, cada sistema de información genera de forma automática una nueva versión asociada al release correspondiente, garantizando trazabilidad, control de cambios y alineación con las buenas prácticas de gestión del ciclo de vida del software.

Este proceso permite mantener un registro actualizado de las versiones desplegadas, facilitando la identificación de los cambios realizados y fortaleciendo la gestión documental técnica de los sistemas de información.

Avances cuarto trimestre:

el equipo de desarrollo culminó la remediación de las vulnerabilidades de alta prioridad que habían quedado pendientes en evaluaciones anteriores, alcanzando así un 100% de cierre de hallazgos críticos identificados durante el año.

Adicionalmente, se llevó a cabo una nueva ronda de pruebas de seguridad sobre aplicaciones recientemente implementadas, incluyendo una segunda auditoría de código y pruebas de penetración controladas en el sistema Ventanilla Única de Trámites ya desplegado. Los resultados de estas evaluaciones mostraron solo hallazgos de criticidad baja, los cuales fueron documentados y se encuentran en proceso de corrección dentro de los ciclos de desarrollo.

Por otro lado, se finalizó la actualización del “Manual de Metodología y Arquitectura de Referencia para el Desarrollo de Sistemas de Información” para incluir formalmente las prácticas DevOps y de desarrollo seguro establecidas durante 2025. De esta manera, al cierre del año la entidad cuenta con un SDLC fortalecido y estandarizado, complementado por herramientas automatizadas en sus pipelines, lo que reduce significativamente el riesgo de introducir vulnerabilidades en el software institucional. Estas prácticas quedan institucionalizadas de cara a 2026, garantizando que la seguridad por diseño siga siendo un pilar en el desarrollo de nuevos sistemas

Riesgo R11 Habilitar y configurar el módulo de auditoría de los SI (aplicaciones, Web Services, Apps. entre otros) acorde con capacidades y necesidades.

Actividad 2: Implementar soluciones de monitoreo centralizado que permitan la recolección, análisis y correlación de eventos de seguridad en tiempo real.

El informe del tercer trimestre estableció que el T3 sería el punto de partida para la ejecución, con el objetivo de “formalizar un procedimiento estándar de implementación de módulos de auditoría” y, a



partir de ahí, "iniciar la actualización y despliegue de dichas capacidades".

El insumo principal para esta tarea es el inventario detallado de sistemas de información, el cual clasifica cada aplicación según su capacidad de auditoría actual. Este inventario distingue claramente entre los sistemas que ya poseen funcionalidades de auditoría (como el Portal Web, SISEG, Intranet y el Buzón de Integridad) y aquellos que operan principalmente en modo "Consulta" y carecen de estos registros (como SIMINERO, SICOM y GEOVISOR).

Es crucial destacar la sinergia entre la mitigación de este riesgo y el riesgo R5. El desarrollo de nuevas aplicaciones bajo el SDLC seguro ha permitido incorporar la auditoría como un requisito desde la concepción del software. Un ejemplo sobresaliente es la nueva "Ventanilla Única de Trámites"; los informes de evidencia muestran capturas detalladas de su módulo de auditoría, que permite visualizar registros de creación, modificación y eliminación, incluyendo comparativas de "antes y después" de los cambios. Esto demuestra que el éxito en la implementación de un desarrollo seguro (R5) acelera directamente el cumplimiento de los objetivos de auditoría (R11) para los nuevos sistemas, materializando el principio de "seguridad por diseño".

Avances del Cuarto Trimestre de 2025

Durante el T3, se han logrado avances significativos en la ejecución de la hoja de ruta definida:

Formalización del Procedimiento Estándar: Se documentó y aprobó el "Procedimiento Estándar para la Implementación de Módulos de Auditoría en Sistemas de Información". Este documento define los requisitos mínimos de registro (quién, qué, cuándo, dónde), los formatos de log estandarizados para facilitar su posterior análisis y las herramientas recomendadas para su implementación en las distintas tecnologías utilizadas en el Ministerio (Java, Python, PHP).

Despliegue de Módulos de Auditoría: Basándose en el inventario y el nuevo procedimiento, se inició el despliegue de capacidades de auditoría en sistemas priorizados. Durante este trimestre, se completó con éxito la implementación del módulo de auditoría en el sistema SIMINERO, que pasó de ser un sistema de "Consulta" a uno con trazabilidad de las consultas y accesos a datos. El desarrollo para el sistema SICOM se encuentra en un 60% de avance y se proyecta su finalización para el inicio del T4.

Actualización del Catálogo de Aplicaciones: Conforme a las conclusiones del análisis previo, se ha documentado formalmente en el catálogo de aplicaciones los sistemas que, por su naturaleza puramente informativa y de no interacción (ej. GEOVISOR), no requerirán un módulo de auditoría transaccional. Esta decisión, con su debida justificación técnica, permite enfocar los recursos en los sistemas que sí manejan datos sensibles o procesos críticos.

Foros Minenergia

Inicio > Foros Minenergia > Forums > Foro de prueba 3 > Histórico

Empiece a escribir para filtrar...

AUTENTICACIÓN Y AUTORIZACIÓN

Grupos [+ Añadir](#)

FOROS MINENERGIA

Comments [+ Añadir](#)

Entitys [+ Añadir](#)

Forums [+ Añadir](#)

Sectors [+ Añadir](#)

Usuarios [+ Añadir](#)

TOKEN DE AUTENTICACIÓN

Tokens [+ Añadir](#)

Histórico de modificaciones: Foro de prueba 3

Choose a date from the list below to revert to a previous version of this object.

OBJECT	FECHA/HORA	COMMENT	CHANGED BY	CHANGE REASON	CHANGES
Foro de prueba 3	5 de Junio de 2025 a las 11:55	Changed	Ninguno	None	• Enddate: 2025-05-18 → 2025-05-30
Foro de prueba 3	14 de Mayo de 2025 a las 14:10	Fecha de creación	Ninguno	None	

2 entradas

Foros Minenergia

Inicio > Foros Minenergia > Comments > Comment by jsromero@minenergia.gov.co on Foro de prueba 3 > Histórico

Empiece a escribir para filtrar...

AUTENTICACIÓN Y AUTORIZACIÓN

Grupos [+ Añadir](#)

FOROS MINENERGIA

Comments [+ Añadir](#)

Entitys [+ Añadir](#)

Forums [+ Añadir](#)

Sectors [+ Añadir](#)

Usuarios [+ Añadir](#)

TOKEN DE AUTENTICACIÓN

Tokens [+ Añadir](#)

Histórico de modificaciones: Comment by jsromero@minenergia.gov.co on Foro de prueba 3

Choose a date from the list below to revert to a previous version of this object.

OBJECT	FECHA/HORA	COMMENT	CHANGED BY	CHANGE REASON	CHANGES
Comment by jsromero@minenergia.gov.co on Foro de prueba 3	5 de Junio de 2025 a las 11:58	Changed	Ninguno	None	• Approved: False → True • Approved at: None → 2025-06-05 16:58:31.774971+00:00 • Approved by: Deleted usuario (pk=None) →
Comment by jsromero@minenergia.gov.co on Foro de prueba 3	5 de Junio de 2025 a las 11:57	Fecha de creación	Ninguno	None	

2 entradas

Imagen 11 . Modulo de auditoria Sección servicio al ciudadano - foros

servicios.minenergia.gov.co/usuarios/entity

Inicio / Administración / Logs

Buscar...

Super Admin

Administración de usuarios y energía

Mostrar 18 de 444 items

ELEMENTO (ID)	ID	FECHA	SERVICIO	NIVEL	MENSAJE
usuario	2025-07-04 20:18	2025-07-04 20:18	Conexiones	3	usuario login from IP 172.17.0.70
usuario	2025-07-04 04:32	2025-07-04 04:32	Conexiones	3	usuario login from IP 172.17.0.70
usuario	2025-06-24 16:26	2025-06-24 16:26	Conexiones	3	usuario login from IP 172.17.0.70
usuario	2025-06-24 16:27	2025-06-24 16:27	Conexiones	3	usuario login from IP 172.17.0.70
usuario	2025-06-20 21:12	2025-06-20 21:12	Conexiones	3	usuario inicio de sesión desde la IP 172.17.0.70
usuario	2025-06-20 16:15	2025-06-20 16:15	Conexiones	3	usuario login from IP 172.17.0.70
usuario	2025-06-19 21:46	2025-06-19 21:46	Conexiones	3	usuario inicio de sesión desde IP 172.17.0.70
usuario	2025-06-18 16:18	2025-06-18 16:18	Conexiones	3	usuario inicio de sesión desde la IP 172.17.0.70
usuario	2025-06-18 16:58	2025-06-18 16:58	Conexiones	3	usuario inicio de sesión desde la IP 172.17.0.70
usuario	2025-06-18 16:58	2025-06-18 16:58	Conexiones	3	usuario inicio de sesión desde la IP 172.17.0.70
usuario	2025-06-17 21:57	2025-06-17 21:57	Conexiones	3	usuario inicio de sesión desde la IP 172.17.0.70
usuario	2025-06-17 19:46	2025-06-17 19:46	Conexiones	3	usuario inicio de sesión desde la IP 172.17.0.70
usuario	2025-06-17 13:47	2025-06-17 13:47	Configuración	4	usuario actualiza un elemento
usuario	2025-06-17 13:48	2025-06-17 13:48	Configuración	4	usuario actualiza un elemento

Mostrando 1 de 444 items

Imagen 12. Modulo de auditoria Gestión de servicios de código abierto- Servicedesk GLPI

Administración Buzón de Transparencia e Integridad

Bienvenido a la Administración Buzón de Transparencia e Integridad

API KEY PERMISSIONS		
API keys	+ Añadir	✎ Modificar
AUTENTICACIÓN Y AUTORIZACIÓN		
Grupos	+ Añadir	✎ Modificar
Usuarios	+ Añadir	✎ Modificar
BUZÓN DE TRANSPARENCIA E INTEGRIDAD		
Asociaciones de Denuncias	+ Añadir	✎ Modificar
Causas del fraude	+ Añadir	✎ Modificar
Ciudades	+ Añadir	✎ Modificar
Denuncias	+ Añadir	✎ Modificar
Departamentos	+ Añadir	✎ Modificar
Entidades	+ Añadir	✎ Modificar
Estados de reporte	+ Añadir	✎ Modificar
Géneros	+ Añadir	✎ Modificar
Involucrados	+ Añadir	✎ Modificar
Observaciones	+ Añadir	✎ Modificar
Perfiles	+ Añadir	✎ Modificar
Respuestas	+ Añadir	✎ Modificar
Roles	+ Añadir	✎ Modificar

Acciones recientes

Mis acciones

- [✎ egonzalezm](#)
Usuario
- [✎ egonzalezm](#)
Usuario
- [✎ cpcorredor](#)
Usuario
- [+ calltech](#)
API key
- [✎ admin](#)
Perfil
- [+ Situación de violencia de género \(SVG\)](#)
Entidad
- [+ Otro](#)
Género
- [+ Masculino](#)
Género
- [+ Femenino](#)
Género
- [+ Prefiero no decirlo](#)
Género

Administración Buzón de Transparencia e Integridad

Bienvenido/a ADMIN VER EL SITIO / CAMBIAR CONTRASEÑA / TERMINAR SESIÓN

Inicio » Buzón de Transparencia e Integridad » Causas del fraude » Disciplinariamente irrelevantes

Enganche a escribir para filtrar...

API KEY PERMISSIONS

API keys [+ Añadir](#)

AUTENTICACIÓN Y AUTORIZACIÓN

Grupos [+ Añadir](#)

Usuarios [+ Añadir](#)

BUZÓN DE TRANSPARENCIA E INTEGRIDAD

Asociaciones de Denuncias [+ Añadir](#)

Causas del fraude [+ Añadir](#)

Ciudades [+ Añadir](#)

Denuncias [+ Añadir](#)

Departamentos [+ Añadir](#)

Entidades [+ Añadir](#)

Estados de reporte [+ Añadir](#)

Géneros [+ Añadir](#)

Modificar Causa del fraude

Disciplinariamente irrelevantes HISTORICO

Nombre de la causa del fraude:

☒ Activa

Fecha de creación: Fecha: Hora: [Ayuda](#)

[GRABAR](#) [Grabar y añadir otro](#) [Grabar y continuar editando](#) [Eliminar](#)

Imagen 13. Modulo de auditoria Buzón de integridad y transparencia



Energía



SISEG
 Sistema de Información de Subsidios para Energía y Gas



Versión 2.6.8

Inicio • Completar Registro Operador • Operador • **Administración •** Normograma • Energía • Dirección Financiera • FOES • GAS • Reportes • Firma Reportes Operador • ANDRES FELIPE ACEVEDO •

Inicio

Bienvenido ANDRES FELIPE ACEVEDO.

SISEG

Sistema de Información de Subsidios de Energía y Gas SISEG

Perfiles
 Usuarios
 Parámetros del sistema
 Políticas de seguridad
 Auditoría
 Listas
 Usuarios Permisionarios 2
 Operaciones
 Configurar UMR
 Consultar TMT
 Usuarios ZNI
 Matriz Defici Año Anterior
 Solicitudes Extemporaneidad 11
 Consultar TMT
 Consultar Base SSPD
 Administración de Glcos

Inicio / Auditoría

Auditoría

Buscar Buscar						
	Usuario	Nombre completo	Acción	Tabla	Fila	Fecha
☐	afacevedo	ANDRES FELIPE ACEVEDO	INGRESAR			2023-12-12 12:41:12 PM
☐	afacevedo	ANDRES FELIPE ACEVEDO	INGRESAR			2023-12-12 10:37:21 AM
☐	afacevedo	ANDRES FELIPE ACEVEDO	INGRESAR			2023-12-06 12:18:36 PM
☐	servicioalcliente@qjenergy.co	JANNETH SANCLEMENTE	ACTUALIZAR	segu_usuario	156	2023-12-06 11:32:21 AM
☐	servicioalcliente@qjenergy.co	JANNETH SANCLEMENTE	CREAR	segu_contrasena	589	2023-12-06 11:32:21 AM
☐	servicioalcliente@qjenergy.co	JANNETH SANCLEMENTE	INGRESAR			2023-12-06 11:31:31 AM

Imagen 14. Módulo de auditoría SISEG.

← ↻ <https://cultura.minenergia.gov.co/admin/apps/section/3/history/>

Administración Cultura Minenergía

Home > Apps > Sections > Encuesta de Cultura 2024 - Cultura Humanista > History

Start typing to filter...

APPS

Questions [+ Add](#)

Responses [+ Add](#)

Sections [+ Add](#)

Subsections [+ Add](#)

Survey completions [+ Add](#)

Surveys [+ Add](#)

AUTHENTICATION AND AUTHORIZATION

Groups [+ Add](#)

Users [+ Add](#)

Change history: Encuesta de Cultura 2024 - Cultura Humanista

DATE/TIME	USER	ACTION
Sept. 25, 2024, 11:39 p.m.	david	Added.
Oct. 4, 2024, 1:34 a.m.	david	Changed Description.
Oct. 4, 2024, 9:34 p.m.	david	Changed Description.
3 entries		

← ↻ <https://cultura.minenergia.gov.co/admin/apps/survey/1/history/>

Administración Cultura Minenergía

Home > Apps > Surveys > Encuesta de Cultura 2024 > History

Start typing to filter...

APPS

Questions [+ Add](#)

Responses [+ Add](#)

Sections [+ Add](#)

Subsections [+ Add](#)

Survey completions [+ Add](#)

Surveys [+ Add](#)

AUTHENTICATION AND AUTHORIZATION

Groups [+ Add](#)

Users [+ Add](#)

Change history: Encuesta de Cultura 2024

DATE/TIME	USER	ACTION
Sept. 25, 2024, 4:19 p.m.	david	Added.
Sept. 25, 2024, 8:03 p.m.	david	Changed Start date.
Oct. 3, 2024, 4:30 p.m.	david	Changed End date.
Oct. 3, 2024, 4:30 p.m.	david	Changed End date.
Oct. 4, 2024, 1:30 a.m.	david	Changed Description.
Oct. 4, 2024, 1:31 a.m.	david	Changed Description.
Oct. 4, 2024, 1:31 a.m.	david	No fields changed.
Oct. 4, 2024, 1:32 a.m.	david	Changed Description.
Oct. 4, 2024, 9:13 p.m.	david	Changed Description.
Oct. 4, 2024, 9:13 p.m.	david	Changed Description.

Imagen 15. Modulo de auditoria Encuesta de medición y cultura organizacional

La siguiente tabla resume el estado actual de la implementación, utilizando el inventario como línea base y reflejando el progreso alcanzado en el T4.

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.

Riesgo R14 Realizar las tareas y actividades de backup, respaldo y disposición acorde con plan de programación y/o solicitudes puntuales.

Actividad 2: Implementar métricas clave como tasas de éxito/falla, capacidad de almacenamiento disponible y tiempos de recuperación, asegurando que el sistema no se sature y opere de manera óptima, esto determinará si se continua con esta herramienta de respaldo o si se debe reemplazar por otra que cumpla los estándares necesarios.

El riesgo R14 se centra en las deficiencias de los procesos de respaldo, que podrían impedir la recuperación de la información y la continuidad de las operaciones ante un incidente. La estrategia de mitigación ha evolucionado de una fase reactiva de estabilización a una fase proactiva de validación y optimización.

El informe del segundo trimestre describía un sistema que se recuperaba de una situación de estrés. Se había liberado una cantidad significativa de espacio (26.3 TB) para poder reanudar los respaldos de activos críticos como los buzones de correo y las bases de datos, que se encontraban represados por saturación de almacenamiento. Además, se había iniciado un proceso a gran escala de Backup Full Granular a Cinta para asegurar una copia de resiliencia a largo plazo.

El tercer trimestre muestra un panorama de mayor control y madurez operativa. El informe de actividades de backup del T3 confirma la consolidación de la operación, con 169 servidores siendo respaldados de manera consistente a disco mediante la herramienta Arcserve UDP. Adicionalmente, se está gestionando activamente la migración de 52 servidores virtuales más desde la infraestructura HyperFlex CISCO hacia un nuevo vCenter XXXX, asegurando la continuidad de la protección durante la transición. Las labores de optimización de almacenamiento también han continuado, con una depuración selectiva que liberó 2.9 TB adicionales, aumentando la holgura operativa y reduciendo el riesgo de futuras saturaciones.

Sin embargo, el avance más significativo de este trimestre ha sido la transición de la simple ejecución de respaldos a la validación empírica de la capacidad de recuperación.

Avances del Cuarto trimestre de 2025: Validación de RTO y RPO

El hito principal del T4 en la gestión de este riesgo fue la ejecución de un ejercicio de restauración controlado, el cual representa la primera validación empírica de los objetivos de recuperación (RTO/RPO) del Ministerio en la vigencia 2025.

- **Activo y escenario:** a solicitud del área técnica, se procedió a restaurar el servidor crítico SXXXPLPRXXXS (IP 172.XX.X.X.XXX).
- **Objetivos del ejercicio:** La prueba tenía un doble propósito: uno táctico, revertir un procedimiento técnico aplicado en la aplicación alojada en el servidor; y uno estratégico, validar la capacidad de cumplir con los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO) establecidos internamente.
- **Ejecución y resultados:** El procedimiento de restauración se gestionó exitosamente, devolviendo el servidor a su estado en el punto de tiempo solicitado. La bitácora técnica del ejercicio, que incluye los tiempos exactos de cada fase de la recuperación, fue registrada y se encuentra en consolidación para el informe final de la prueba.

Este ejercicio de restauración exitoso es un logro que trasciende la gestión técnica de backups. Representa un activo estratégico para la entidad por varias razones:

1. **Genera confianza institucional:** Demuestra de manera irrefutable la capacidad del Grupo TIC para recuperar sistemas críticos, pasando de la confianza basada en la fe a la confianza basada en la evidencia.
2. **Proporciona datos para el DRP:** Los tiempos reales medidos durante la restauración (el RTO real) y la precisión del punto de datos recuperado (el RPO real) son insumos invaluable para actualizar y refinar el Plan de Recuperación ante Desastres (DRP) asociado al riesgo. Transforma el DRP de un documento teórico a un plan probado y creíble.
3. **Establece una metodología replicable:** El proceso seguido para la restauración del servidor SXXXXXLPRXXXXXS sirve como un modelo validado que ahora puede ser replicado de manera sistemática en otros sistemas críticos, estableciendo un programa de pruebas de recuperación continuo y basado en evidencia.



Imagen 16 . Evaluación y avance del proceso de backup general de cinta UDP.

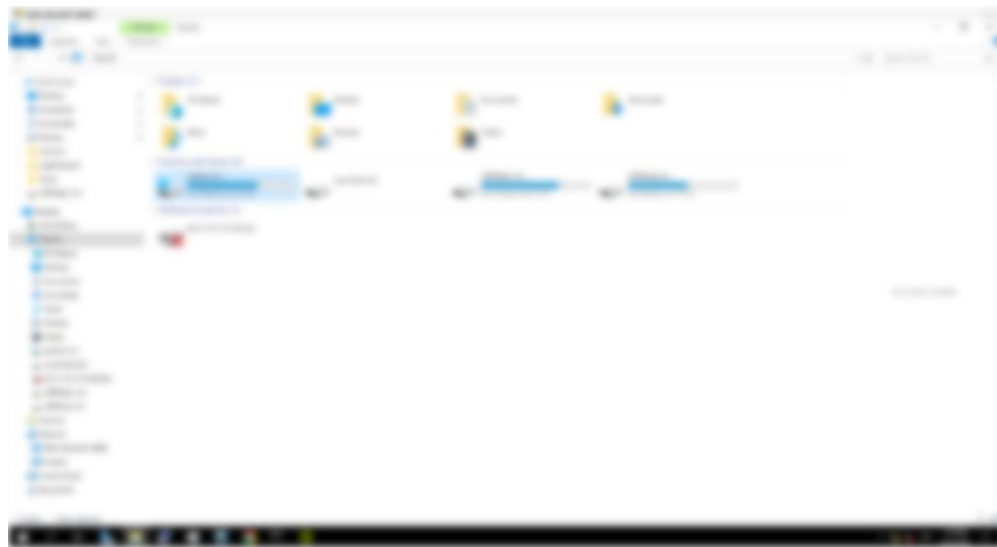


Imagen 17. Repositorio y muestra de espacio de almacenamiento de la infraestructura

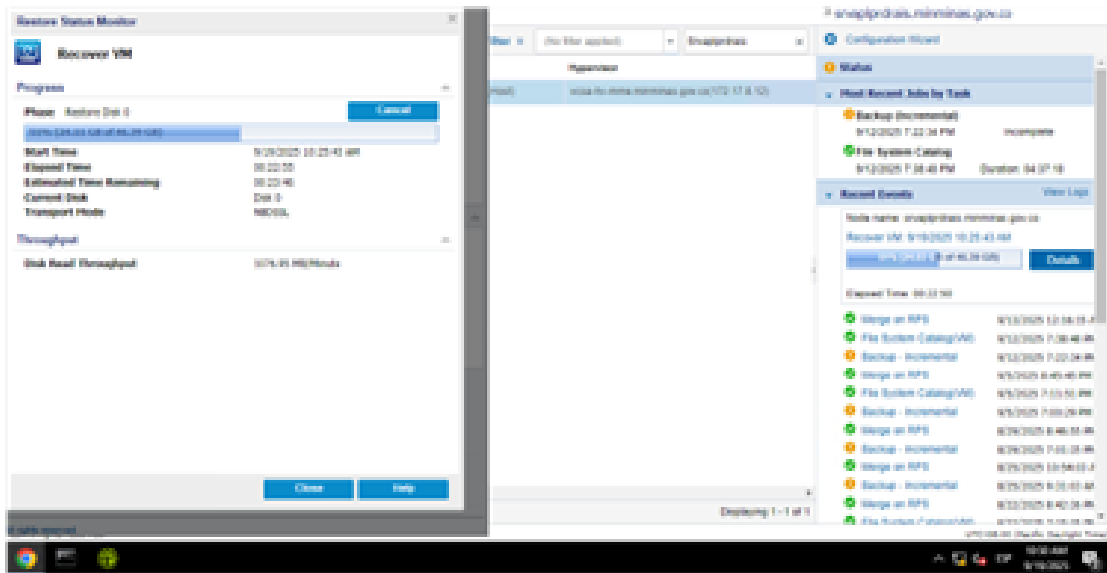


Imagen 18 Proceso de arcservbackup y servidores en proceso



Imagen 19 . Muestreo y lista de proceso de backup.

Nota: si se desea saber más información e informe completo comunicarse con el oficial de seguridad de la información de la entidad.

Riesgo R21 Falencias en la clasificación de activos de información y R23 gestión del continuidad del negocio y recuperación ante desastres DRP

Contexto de los riesgos interconectados y estrategia de mitigación

Avances del Cuarto trimestre de 2025: La Institucionalización de la gestión de activos y continuidad

El avance más determinante del T4 para estos riesgos fue la emisión de una circular oficial por parte de la Secretaría General, dirigida a todas las direcciones, subdirecciones y jefaturas del Ministerio. Este documento es la evidencia clave que formaliza y mandata las acciones necesarias para mitigar los riesgos R21 y R23.

- **Mandato Institucional:** La circular establece la necesidad de actualizar el Inventario de Activos de Información, los BIA y los BCP como un requisito derivado del Manual Operativo del MIPG, la norma ISO/IEC 27001:2022 y los lineamientos del MSPI de MINTIC. Esto eleva la tarea de una iniciativa del Grupo TIC a una obligación institucional.
- **Creación de estructuras de gobernanza:** El documento ordena la conformación de dos mesas de trabajo clave: la "Mesa de Seguridad y Privacidad de la Información" y la "Mesa de Gestión de Continuidad del Negocio". Estas mesas servirán como los foros para coordinar y ejecutar las actividades.
- **Asignación de responsabilidades claras:** La circular exige a cada dependencia del Ministerio designar formalmente dos roles cruciales antes del 24 de septiembre:
 1. Un **enlace (y su respaldo)**, responsable de diligenciar la matriz del Inventario de Activos de Información de su área, bajo la coordinación del Grupo TIC.
 2. Un **responsable para la actualización de los BIA y BCP**, encargado de participar en las mesas de trabajo, levantar los requerimientos de continuidad y participar en pruebas y simulacros.
- **Actualización de la Infraestructura del DRP:** Paralelamente a estos avances en gobernanza, se ha continuado con el proceso contractual para la adquisición de la nueva herramienta de respaldo con almacenamiento inmutable y replicación automática, así como el traslado del centro de datos alternativo a una instalación de colocation externa. Estas acciones, iniciadas en el T3, constituyen la base tecnológica sobre la cual se construirá el DRP actualizado.

Nota: para mayor información del proceso de avance se requiere informar la oficial de seguridad

4.4 GESTIÓN DE POLÍTICAS Y PROCEDIMIENTOS

Durante el cuarto trimestre de 2025, se culminaron las actividades de ajuste y modernización del marco normativo del Sistema de Gestión de Seguridad de la Información (SGSI) que se venían adelantando desde comienzos de año. Un logro principal fue finalizar la propuesta de modificación de la Resolución 40644 (norma que rige la política de seguridad y privacidad de la información en el Ministerio). Esta modificación propuesta -lista para ser elevada a aprobación de la alta dirección al cierre del año- busca desligar las políticas de seguridad del pesado proceso de expedición formal a nivel de resolución, permitiendo realizar ajustes y actualizaciones de manera mucho más eficiente e inmediata. En términos prácticos, una vez adoptada, esta medida agilizará la capacidad del Ministerio para responder normativamente a nuevas amenazas o lineamientos, ya que las políticas internas de seguridad podrán ser actualizadas sin requerir cada vez una nueva resolución ministerial.

En paralelo, se consolidó la actualización de varios documentos y guías clave del SGSI. Continuando con los esfuerzos previos, se ajustó formalmente el Manual de Usuario de SICOM, incorporando directrices claras sobre la aplicación de la política de privacidad y protección de datos personales en la plataforma SICOM, en estricto cumplimiento de la Ley 1581 de 2012. De igual modo, se concluyó la revisión integral de la Política de Uso Responsable de Inteligencia Artificial y se definió una plantilla estándar para el Informe de Incidentes Cibernéticos. Estos tres productos (el manual ajustado, la política de IA actualizada y la nueva plantilla de informes) conforman un marco documental renovado y más completo, adaptado a las necesidades actuales de la entidad. Al cierre del cuarto trimestre, dichos documentos se encontraban en trámite de aprobación formal; se espera su expedición y difusión durante el primer trimestre de 2026, lo que asegurará su plena implementación en toda la entidad.

Por otra parte, se logró institucionalizar mejoras en el proceso de gestión de incidentes de seguridad de la información. Particularmente, durante este trimestre se terminó de implementar la nueva plantilla oficial de reporte de incidentes cibernéticos (mencionada anteriormente) y se realizaron pruebas piloto de su uso por parte de los equipos técnicos. Esta herramienta unificada para reportar incidentes permitirá estandarizar la documentación de cualquier incidente de seguridad ocurrido, mejorando la trazabilidad de los eventos, facilitando el análisis forense cuando sea necesario y en general optimizando la toma de decisiones basada en evidencia frente a incidentes de seguridad. Se prevé que, tras la aprobación formal de la plantilla, su uso se vuelva obligatorio y rutinario en 2026 para todo incidente que se presente.

Adicionalmente, se avanzó en la estructuración del proceso de gobernanza de dispositivos tecnológicos asignados a las dependencias. Con el objetivo de establecer un control centralizado sobre los equipos institucionales (computadores portátiles, estaciones de trabajo, periféricos, etc.), se diseñó un procedimiento preliminar que establece que todo nuevo equipo de cómputo debe ser gestionado y validado por la Dirección TIC antes de su asignación al usuario final. Durante el cuarto trimestre se comenzó a aplicar esta directriz para los equipos adquiridos recientemente, lo que permitió afinar el proceso. Esta medida asegura un control más riguroso sobre los activos tecnológicos, garantizando que cada equipo entregado cumpla con una configuración básica de seguridad (ej. instalación de software de protección, configuración de contraseñas robustas, parches al día) y quede registrado para su seguimiento en el inventario central. Con ello, se fortalece la gestión

del ciclo de vida de los activos TI y se mejora la visibilidad sobre su ubicación y estado de seguridad dentro del ecosistema institucional.

Todos estos avances se enmarcan en el proceso de mejora continua del SGSI y dejan al Ministerio en una posición normativa mucho más sólida al finalizar 2025. Las políticas y procedimientos de seguridad de la información han sido revisados y actualizados en su mayoría, y existen mecanismos más ágiles para su futura modificación conforme cambie el panorama de riesgos o surjan nuevos requerimientos legales. El reto inmediato para el primer trimestre de 2026 será obtener la aprobación final y difundir ampliamente estos nuevos documentos normativos (políticas, manuales y procedimientos) para asegurar su apropiación por parte de todos los funcionarios y contratistas. De esta forma, la gestión de la seguridad de la información contará con un marco normativo robusto y actualizado, alineado con estándares internacionales y buenas prácticas, que apoyará las demás iniciativas técnicas y organizacionales emprendidas.

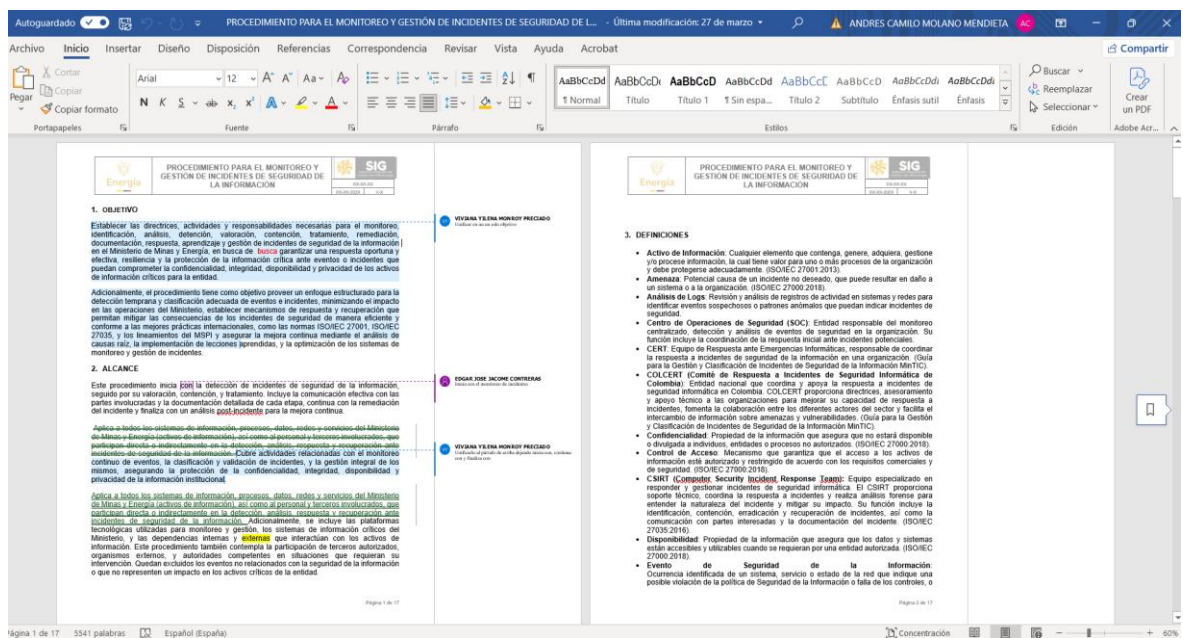


Imagen [21]. Control de cambios y observaciones del procedimiento de monitoreo y gestión de incidentes de seguridad de la información.

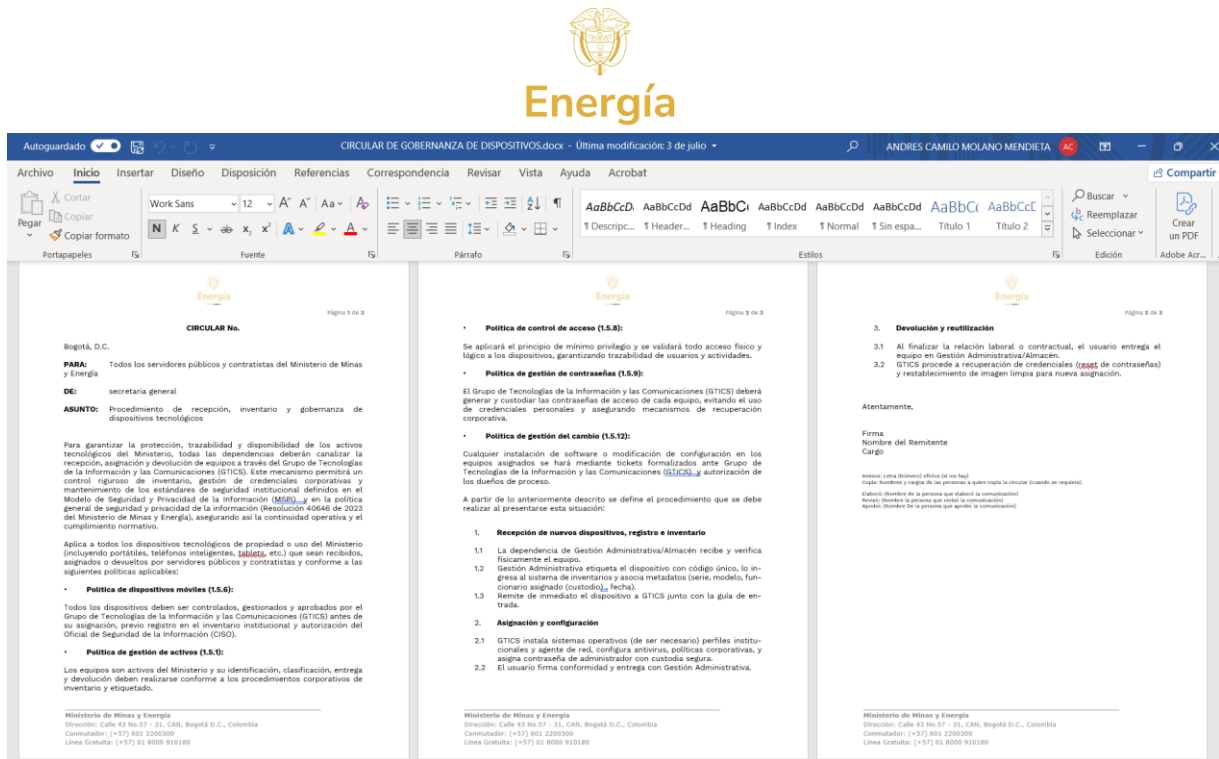


Imagen [22]. Circular estructurada para el manejo y gobernanza de la los dispositivos TI .

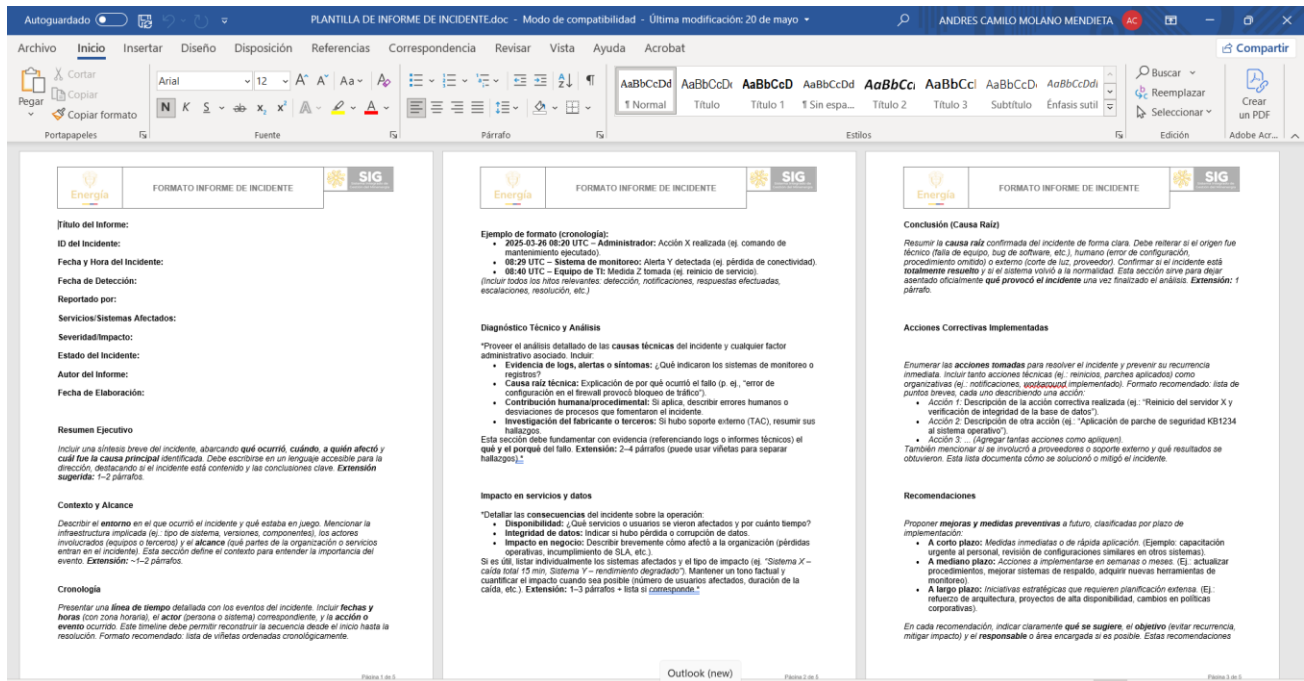


Imagen [23]. Plantilla de informe de gestión de incidentes.

Ministerio de Minas y Energía

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

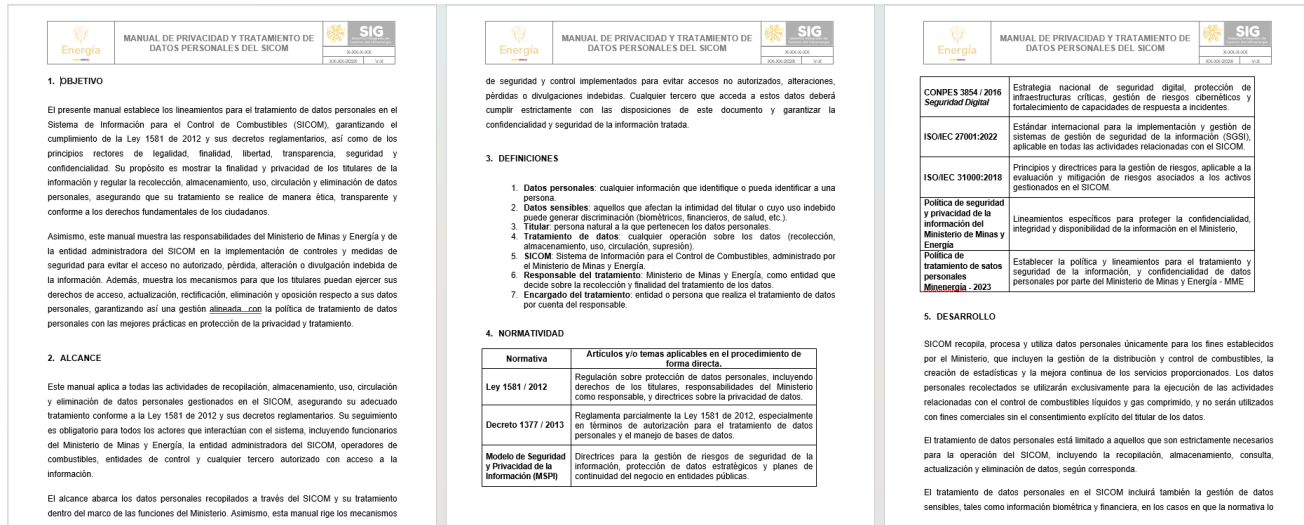


Imagen [24]. Manual de uso y tratamiento de datos personales de SICOM

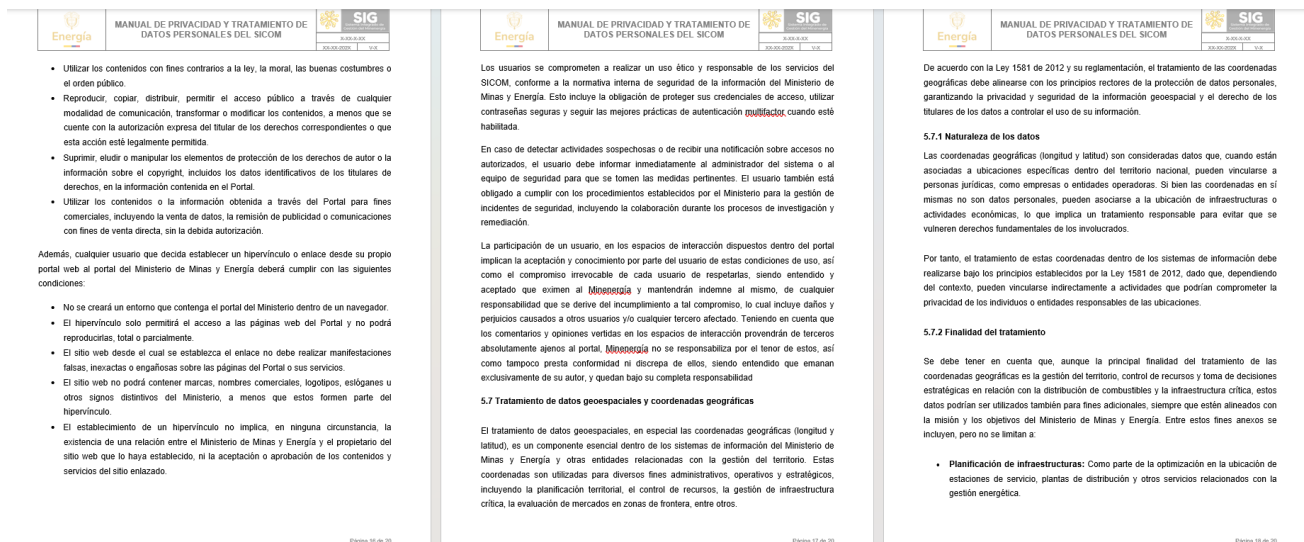


Imagen [25]. Manual de uso y tratamiento de datos personales de SICOM

4.5 GESTIÓN DE RECURSOS DE SEGURIDAD

Conforme al análisis del contexto actual de la entidad, tanto en su dimensión externa marcada por la evolución de amenazas cibernéticas emergentes, como los ataques dirigidos, el ransomware y la ingeniería social como en su dimensión interna, donde persisten retos en materia de protección de datos, madurez en seguridad de la información y cultura organizacional en ciberseguridad, se ha definido una hoja de ruta estratégica de proyectos prioritarios para la vigencia 2025. Estos proyectos están diseñados para cerrar brechas críticas de seguridad, mejorar los niveles de preparación ante

incidentes, y fortalecer los pilares institucionales de ciberdefensa, ciberseguridad y ciberresiliencia, en línea con las directrices del Gobierno Digital y las políticas nacionales de confianza digital.

Tabla 4.
Proyectos a implementar vigencia 2025

PROYECTO
Contratar los servicios especializados para realizar análisis de vulnerabilidades, ethical hacking e pentesting social a la infraestructura tecnológica del Ministerio de Minas y Energía
Implementar soluciones de seguridad y privacidad de la información que incorpore procesos, talento humano y tecnología para dar cumplimiento a los lineamientos de MINTIC.
Implementar un Csirt para responder a incidentes de seguridad que incorpore procesos, recurso humano y tecnología para dar cumplimiento a la política de gobierno digital en el habilitador de seguridad digital.
Implementar esquemas de continuidad de negocio (BCP — Business Continuity Plan) y plan de recuperación de desastres (DRP) sectorial, que incorpore procesos, recurso humano y tecnología
Adquirir herramienta de seguridad para el monitoreo de la red, para detección de amenazas en tiempo real en el Ministerio de Minas y Energía (SOC)
Renovar el licenciamiento de firewall local y adquisición de firewall de aplicaciones web (WAF) para proteger las aplicaciones web y monitorizar el tráfico HTTP del centro de datos alterno del Ministerio de Minas y Energía

El Ministerio ha definido una hoja de ruta clara con seis grandes proyectos estratégicos para 2025, detallados en la Tabla 4. Estos incluyen la contratación de servicios de hacking ético, la implementación de un CSIRT, el desarrollo de un DRP/BCP, la creación de un SOC y la renovación de firewalls y WAF. Para el tercer trimestre, se ha logrado un avance significativo en el proceso de contratación para cada uno de estos proyectos de inversión, superando la parálisis "precontractual" y avanzando hacia la etapa final de adjudicación e inicio pertinente.

Con esta transición de la planificación a la ejecución, las expectativas para el cuarto trimestre se centran en el inicio tangible de las actividades de implementación y seguimiento. Específicamente,



se espera poder realizar el seguimiento de la infraestructura del Centro de Monitoreo Sectorial, comenzar la implementación de los nuevos controles y lineamientos del proyecto MSPI 2025, y ejecutar las pruebas pertinentes en el proyecto de *ethical hacking*, incluyendo un ejercicio profundo de ingeniería social. Este avance representa un punto de inflexión crucial, transformando la estrategia de seguridad de un plan en papel a un programa con proyectos activos y resultados medibles.

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

5.1 GESTIÓN DE INDICADORES

La gestión de indicadores constituye una herramienta clave para evaluar la eficacia, eficiencia y efectividad de las políticas, procedimientos y controles establecidos en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) del Ministerio de Minas y Energía. Esta práctica permite no solo monitorear el cumplimiento normativo, sino también identificar oportunidades de mejora continua, en concordancia con los principios establecidos en la Guía Técnica No. 9 del Modelo de Seguridad y Privacidad de la Información (MSPI) y las normas internacionales ISO/IEC 27001:2022 y ISO/IEC 27004:2022.

Durante el cuarto trimestre de 2025, se realizó una revisión de los indicadores previamente definidos en la vigencia anterior, con el objetivo de priorizar aquellos que mejor reflejaran la madurez del sistema, la capacidad de respuesta institucional y el impacto en la cultura de seguridad. Tras una evaluación conjunta con los equipos técnicos y el responsable de seguridad de la información, se seleccionaron cinco indicadores clave para su seguimiento durante el año. Esta selección responde tanto a las prioridades institucionales como a la necesidad de contar con métricas claras que reflejen los avances logrados.

A continuación, se presenta la tabla con los indicadores seleccionados, sus descripciones, fórmulas y los resultados correspondientes al cuarto trimestre de 2025:

Tabla 5
Resultado de indicadores de seguridad de la información

Indicador	Definición	Fórmula	Meta	Meta	Resultado 2 trimestre	Actividad
-----------	------------	---------	------	------	-----------------------	-----------

SGIN01	Organización de Seguridad de la Información	Mide el nivel de compromiso institucional con la definición formal de roles y responsabilidades en seguridad de la información.	(Roles definidos / Roles requeridos) * 100	80%-90% satisfactorio, 100% sobresaliente	100% (3/3)	Se definieron formalmente los cargos de CISO mediante la designación de la responsabilidad por parte de la coordinación del grupo TICS.
SGIN03	Tratamiento de eventos de seguridad	Evalúa la eficiencia en la gestión de los incidentes de seguridad detectados.	(Eventos tratados / Eventos reportados) * 100	80%-90% satisfactorio, 100% sobresaliente	100% (NA/NA)	Sin incidentes
SGIN16	Implementación de controles	Mide el grado de implementación de controles de seguridad según el plan de tratamiento de riesgos.	(Controles implementados / Controles planificados) * 100	75%-80% mínimo, 100% sobresaliente	40% (3/7)	Una actividad de control por cada riesgo fue implementada en este trimestre. Ver informe de seguimiento.
SGIN15	Disponibilidad de servicios críticos	Porcentaje de tiempo que los sistemas críticos estuvieron operativos según los Acuerdos de Nivel de Servicio (ANS).	(Tiempo disponible / Tiempo planificado) * 100	>89% sobresaliente	100%	Falla en la disponibilidad del servicio de internet.
SGIN04	Sensibilización en seguridad de la información	Evalúa la efectividad del plan de sensibilización mediante actividades ejecutadas frente a las programadas.	(Eventos realizados / Eventos programados) * 100	80%-90% satisfactorio, 100% sobresaliente	100% (7/7)	7 sesiones Sensibilización y capacitación

El resultado de los indicadores seleccionados evidencia un desempeño sobresaliente durante el primer trimestre, cumpliendo al 100% con las metas propuestas en todos los frentes evaluados. Este desempeño refleja el compromiso de la entidad con el fortalecimiento de su SGSI, la implementación oportuna de controles, la estructuración formal de roles de seguridad y la eficiencia en la atención de incidentes.

5.2 GESTIÓN DE VULNERABILIDADES.

El Cuarto trimestre de 2025 marcó un período de transición y fortalecimiento para el ciclo de vida de la gestión de vulnerabilidades. Si bien el proceso formal de seguimiento a través de la herramienta



Planner se mantuvo, el foco principal del trimestre se desplazó hacia la consolidación del proceso a raíz de un cambio significativo en los custodios y responsables de los sistemas de información e infraestructura. Esta reestructuración organizacional requirió un esfuerzo concentrado en la capacitación y alineación de los nuevos actores para garantizar la continuidad y eficacia del programa a largo plazo.

Las actividades del trimestre se centraron en capacitar a los nuevos responsables sobre sus roles dentro del flujo de trabajo de gestión de vulnerabilidades. Se llevaron a cabo sesiones intensivas para asegurar que cada custodio comprendiera a cabalidad el procedimiento, desde la notificación inicial hasta el cierre. Se hizo especial hincapié en la importancia de utilizar el formato oficial para documentar las acciones de remediación, la necesidad de adjuntar evidencias claras y suficientes que demuestren la corrección de la brecha, y la obligación de establecer y cumplir rigurosamente los tiempos de respuesta acordados, particularmente para las vulnerabilidades de criticidad alta.

Este enfoque en la capacitación y la adopción del proceso tuvo un impacto directo en las métricas de remediación del trimestre, ya que la prioridad fue asegurar una base de conocimiento sólida en lugar de la ejecución inmediata de correcciones. Conscientes de esta situación, se tomó la decisión estratégica de realizar un ajuste fundamental en la planificación: al inicio del cuarto trimestre se llevará a cabo un nuevo escaneo exhaustivo de vulnerabilidades en toda la infraestructura tecnológica. Esta medida permitirá establecer una nueva línea de base completa y actualizada del estado de seguridad de la entidad.

Este re-escaneo integral servirá como punto de partida para el nuevo ciclo operativo, asegurando que los equipos, ahora debidamente capacitados, trabajen sobre la base de la información más reciente y precisa. La expectativa para el cuarto trimestre es que, con un proceso robustecido y responsabilidades claramente asimiladas, la tasa de remediación de vulnerabilidades, especialmente las críticas, mejore significativamente, demostrando el valor de la inversión en la capacitación y consolidación del proceso realizada durante este período de transición.

5.3 PLAN DE AUDITORÍAS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la auditoría interna realizada durante el tercer trimestre de 2025, se consolidaron los hallazgos y oportunidades de mejora que dieron origen a la formulación de planes de mejora específicos, con acciones concretas, responsables definidos y tiempos de ejecución. Estos planes fueron estructurados de manera articulada con la Oficina de Planeación y Gestión, garantizando coherencia con el enfoque institucional de mejora continua, y asegurando que los ajustes propuestos respondan tanto a los lineamientos del SGSI como a los requerimientos estratégicos del Ministerio.



De esta forma, la auditoría no se asumió únicamente como un ejercicio de verificación, sino como un punto de partida para fortalecer la gobernanza, el control y la trazabilidad de la seguridad y privacidad de la información.

En el marco de dicho plan de mejora, se definieron acciones pertinentes que se incorporaron de manera formal al plan de trabajo del equipo de Seguridad y Privacidad de la Información, priorizando aquellas orientadas al cierre de brechas estructurales identificadas en la auditoría. Entre estas acciones se incluyen el fortalecimiento del inventario y clasificación de activos de información, la alineación de la gestión de riesgos con los activos y procesos críticos, y la consolidación de los mecanismos de seguimiento y evidencias de implementación, de manera que el avance pueda ser verificado y auditado de forma objetiva. Este enfoque permite mantener una gestión basada en resultados, con seguimiento periódico y retroalimentación, asegurando que cada hallazgo tenga respuesta institucional documentada y verificable.

Adicionalmente, las acciones derivadas de la auditoría se articularon con el plan de cierre de brechas del FURAG, con una proyección estratégica hacia el año 2026, de manera que el Ministerio asegure consistencia entre la operación del SGSI, la mejora institucional y los compromisos de desempeño en gestión pública. En este sentido, el plan de auditorías y los planes de mejora se convierten en insumos para la planeación 2026, permitiendo establecer prioridades, metas y entregables trazables en el marco del fortalecimiento de la seguridad digital.

6. CAPACITACIÓN Y SENSIBILIZACIÓN

Durante el cuarto trimestre de 2025 se fortaleció de manera significativa el componente de capacitación y sensibilización en seguridad y privacidad de la información, mediante la ejecución de siete (7) charlas orientadas a elevar la cultura de seguridad digital en los funcionarios, contratistas y equipos con roles críticos. Estas actividades se diseñaron con un enfoque preventivo y de reducción de riesgo, priorizando amenazas frecuentes y de alto impacto para la entidad, tales como la suplantación, el robo de credenciales y los fraudes digitales. En conjunto, las sesiones permitieron reforzar hábitos seguros, mejorar la capacidad de reconocimiento de señales de alerta y promover comportamientos de reporte oportuno, contribuyendo de forma directa al fortalecimiento del SGSI.

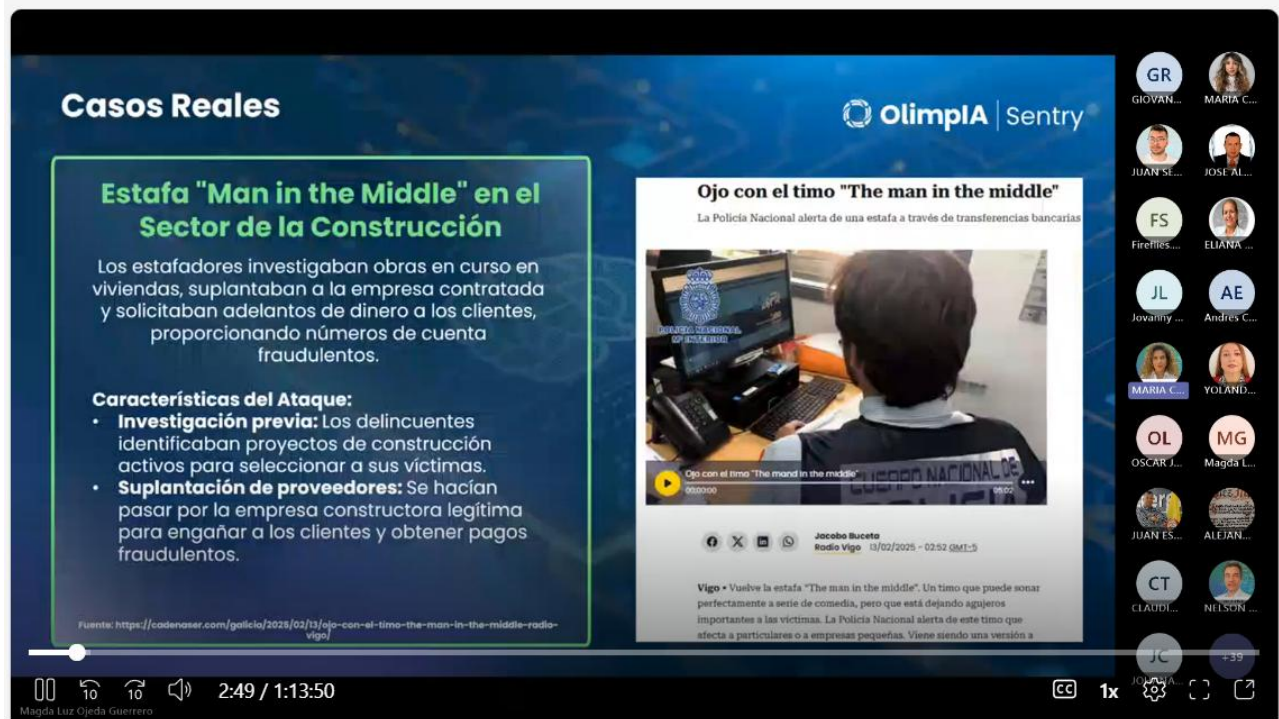
Como hito central del trimestre, cinco (5) de las siete charlas se desarrollaron en el marco del Mes de la Seguridad y Privacidad de la Información, realizado en octubre, consolidando un espacio institucional de sensibilización masiva y apropiación de buenas prácticas. Para esta agenda se contó con conferencistas externos, lo cual permitió enriquecer los contenidos con perspectivas especializadas, casos reales y tendencias actuales del panorama de amenazas, fortaleciendo el impacto pedagógico. Estas jornadas, además de promover la participación activa, funcionaron como un mecanismo de alineación transversal entre dependencias, ayudando a homogeneizar criterios institucionales sobre protección de información, gestión de incidentes y autocuidado digital.

Adicionalmente, durante el mes de noviembre se ejecutaron dos (2) charlas complementarias,

enfocadas específicamente en el aumento de casos de estafas digitales, suplantación de identidad y modalidades de engaño dirigidas a servidores públicos. Estas sesiones se orientaron a fortalecer la capacidad de prevención y respuesta ante escenarios como llamadas fraudulentas, correos engañosos y técnicas de persuasión empleadas para obtener accesos indebidos. El enfoque buscó no solo sensibilizar, sino también habilitar a los asistentes con criterios prácticos para identificar patrones de ataque, validar comunicaciones sospechosas y activar las rutas de reporte definidas por el Ministerio.

En paralelo a la formación, el Ministerio desarrolló dos (2) ejercicios dirigidos de phishing como mecanismo de medición y fortalecimiento del factor humano. Los escenarios simulados abordaron temáticas de alto realismo relacionadas con proveedores comerciales y supuestas caídas de servicios en la nube, orientadas a inducir el ingreso de credenciales institucionales. Estos ejercicios permiten identificar brechas de comportamiento, segmentar necesidades de refuerzo y ajustar el plan de sensibilización con base en evidencia. Asimismo, se adelanta un ejercicio de ingeniería social física (presencial) que actualmente se encuentra en ejecución; a la fecha de cierre del informe aún no cuenta con resultados finales, dado que el proceso está pendiente de cierre y consolidación de hallazgos.

martes, 14 octubre 2025 10:17 a. m. - 11:31 a. m.



Casos Reales

Estafa "Man in the Middle" en el Sector de la Construcción

Los estafadores investigaban obras en curso en viviendas, suplantaban a la empresa contratada y solicitaban adelantos de dinero a los clientes, proporcionando números de cuenta fraudulentos.

Características del Ataque:

- **Investigación previa:** Los delincuentes identificaban proyectos de construcción activos para seleccionar a sus víctimas.
- **Suplantación de proveedores:** Se hacían pasar por la empresa constructora legítima para engañar a los clientes y obtener pagos fraudulentos.

Fuente: <https://cadenaser.com/galicia/2025/02/13/ojo-con-el-timo-the-man-in-the-middle-radio-vigo/>

Ojo con el timo "The man in the middle"
La Policía Nacional alerta de una estafa a través de transferencias bancarias

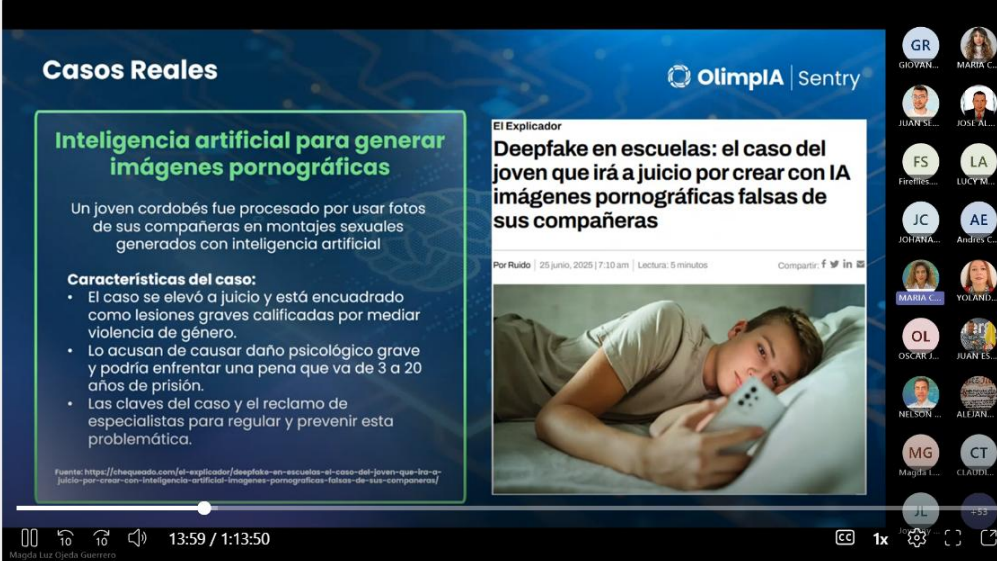
Video player controls: 2:49 / 1:13:50

Participants list:

- GR GIOVAN...
- MARIA C...
- JUAN SE...
- JOSE AL...
- FS Fireflies...
- ELIANA ...
- JL Jovanny ...
- AE Andres C...
- MARIA C...
- YOLAND...
- OL OSCAR J...
- MG Magda L...
- JUAN ES...
- ALEJAN...
- CT CLAUDI...
- NEILSON ...
- JC JOSEPH ...

Imagen [26]. Charla Mes de seguridad de la información- 1 sesión

martes, 14 octubre 2025 10:17 a. m. - 11:31 a. m.



Casos Reales

Inteligencia artificial para generar imágenes pornográficas

Un joven cordobés fue procesado por usar fotos de sus compañeras en montajes sexuales generados con inteligencia artificial

Características del caso:

- El caso se elevó a juicio y está encuadrado como lesiones graves calificadas por mediar violencia de género.
- Lo acusan de causar daño psicológico grave y podría enfrentar una pena que va de 3 a 20 años de prisión.
- Las claves del caso y el reclamo de especialistas para regular y prevenir esta problemática.

Fuente: <https://chiquitaco.com/el-explicador/deepfake-en-escuelas-el-caso-del-joven-que-ira-a-juicio-por-crear-con-inteligencia-artificial-imagenes-pornograficas-falsas-de-sus-companeras/>

El Explicador

Deepfake en escuelas: el caso del joven que irá a juicio por crear con IA imágenes pornográficas falsas de sus compañeras

Por Ruido | 25 junio, 2025 | 7:10 am | Lectura: 5 minutos

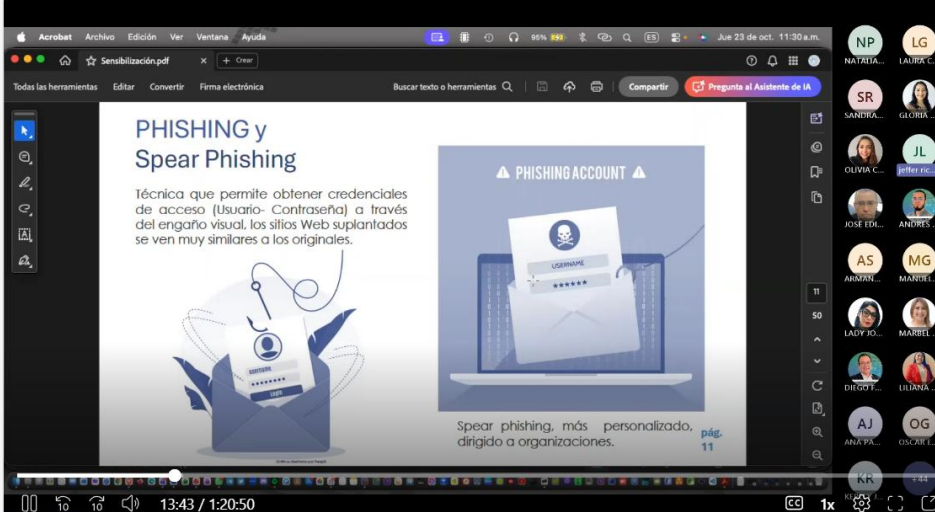
Compartir: f w in

13:59 / 1:13:50

Imagen [27]. Charla Mes de seguridad de la información, 2 sesión

jueves, 23 octubre 2025 11:17 a. m. - 12:37 p. m.

Parte 1 Parte 2



PHISHING y Spear Phishing

Técnica que permite obtener credenciales de acceso (Usuario- Contraseña) a través del engaño visual, los sitios Web suplantados se ven muy similares a los originales.

PHISHING ACCOUNT

Spear phishing, más personalizado, dirigido a organizaciones.

pág. 11

13:43 / 1:20:50

Imagen [28]. Charla Mes de seguridad de la información, 3 sesión

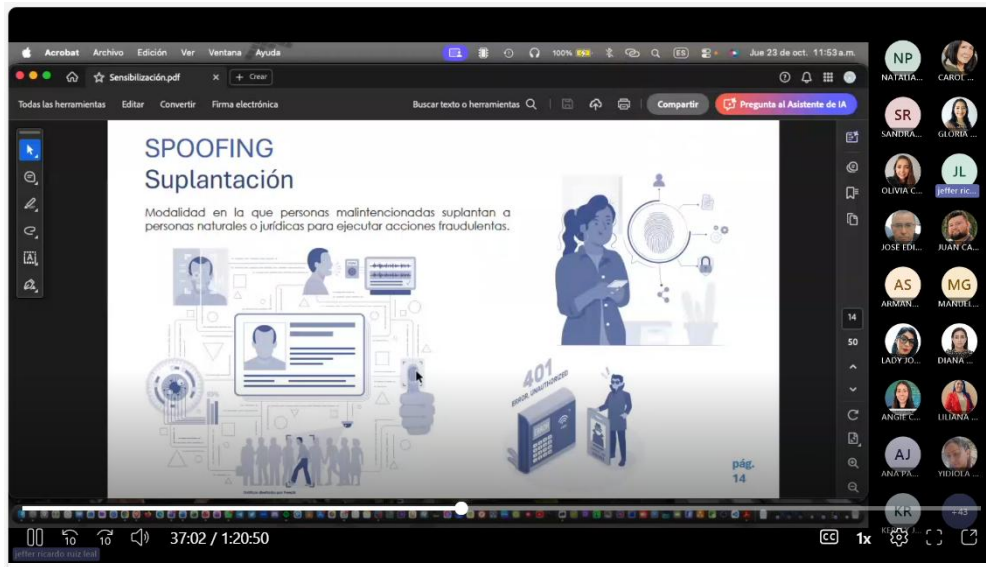


Imagen [29]. Charla Mes de seguridad de la información, 4 sesión



Imagen [30]. Charla Mes de seguridad de la información, 5 sesión

martes, 4 noviembre 2025 9:13 a. m. - 10:11 a. m.

Por que son Importantes y por que deberiamos usarlas

Las **bóvedas cibernéticas** son importantes porque **protegen la información digital más valiosa de personas y organizaciones** frente a los riesgos de un ataque digital. Las bóvedas cibernéticas son herramientas digitales que nos ayudan a **proteger, organizar y asegurar nuestra información**.

Hoy en día, casi toda nuestra vida está conectada a Internet (cuentas bancarias, redes sociales, fotos, documentos, correos, etc) y eso nos hace vulnerables a robos y ataques cibernéticos.

Usar una bóveda cibernética es una forma práctica y segura de cuidar nuestros datos.

-  **Protegen contra el robo de información**
-  **Ayudan a mantener la privacidad**
-  **Facilitan la organización y el acceso seguro**
-  **Previenen pérdidas de información**
-  **Son una defensa clave contra ciberataques**




21:32

21:32 / 57:42
1x

Imagen [31]. Charla Mes de seguridad de la información, 6 sesión

#Socialización Conoce las medidas para garantizar tu tranquilidad en las compras 🛒 decembrinas 🎄 : reunión

Evento Asistente para programación

Unirse
RSVP
Provisional
15 minutos antes
Clasificar
Privado
Aplicaciones





**Protocolo de compras en línea:
Guía para identificar estafas
y otras pesadillas de temporada**

Reconoce y toma las medidas necesarias para
garantizar tu tranquilidad en estas fiestas.

Miércoles **26** **2:00** p.m.
noviembre

Modalidad: Virtual vía Teams

La Energía de Nuestra Gente 

Seguimiento

Organizador

 Vivo Minenergía
Enviado el Martes, 25/11/2025 a las 5:09 PM

Asistentes

No respondió

✓ Sin respuesta: 2

 Funcionarios Mine... Obligatorio

 Contratistas Minen... Obligatorio

Microsoft Teams [¿Necesita ayuda?](#)

Imagen [32]. Charla Mes de seguridad de la información, 7 sesión



Energía

