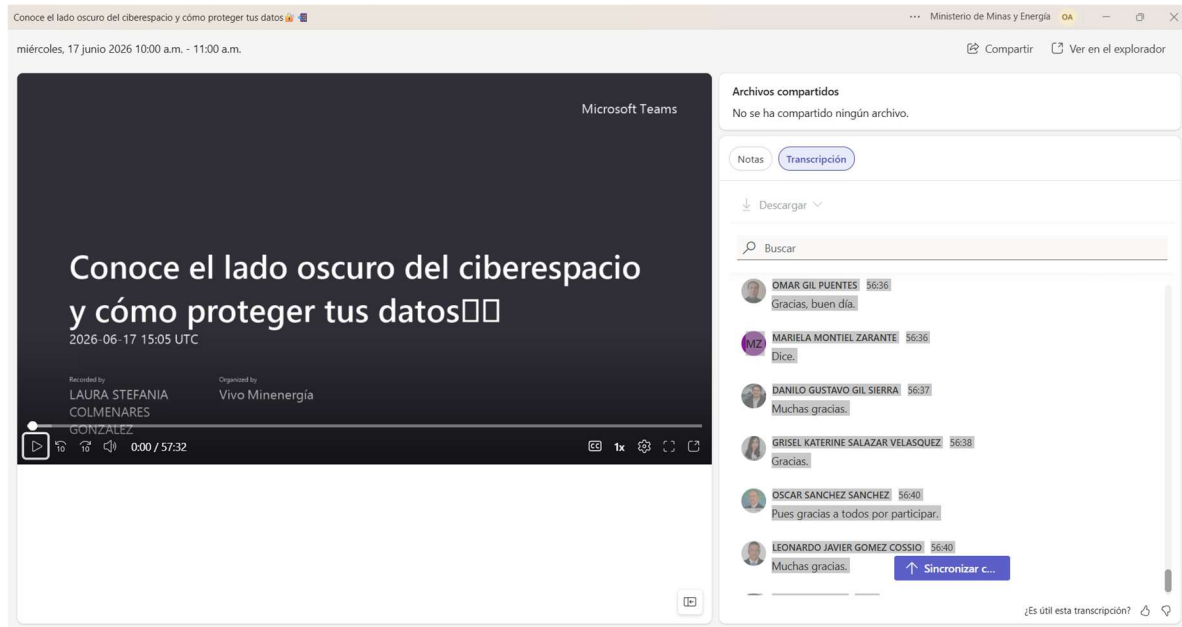


FECHA: 17 DE JUNIO DE 2026

Nombre de la capacitación: Ciberespacio, amenazas cibernéticas y buenas prácticas de ciberseguridad

Facilitadores: Danilo Gustavo Gil Sierra y Laura Stefanía Colmenares González

Participantes: Funcionarios y contratistas del Ministerio de Minas y Energía.



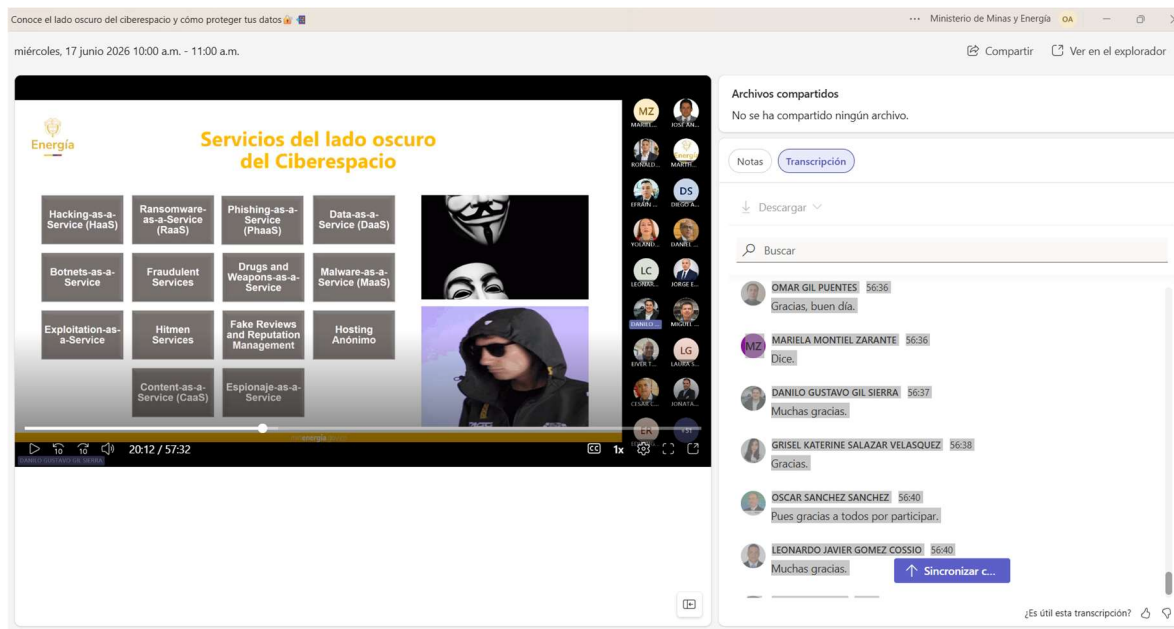
Objetivo

Fortalecer los conocimientos de los servidores y colaboradores del Ministerio sobre los conceptos fundamentales del ciberespacio, las amenazas cibernéticas más frecuentes y las medidas preventivas que permiten proteger la información institucional y personal durante el uso de las tecnologías de la información y las comunicaciones.

Desarrollo

La capacitación inició con una introducción al concepto de **ciberespacio**, entendido como un entorno digital dinámico e interconectado, conformado por redes, sistemas de información, dispositivos, plataformas y servicios que permiten el intercambio permanente de datos a nivel mundial. Se explicó que, debido a su naturaleza global y a la ausencia de fronteras físicas, el ciberespacio constituye un escenario en permanente evolución que ofrece múltiples oportunidades para el desarrollo de las actividades institucionales, pero que también expone a las organizaciones y a las personas a diversos riesgos de seguridad informática.

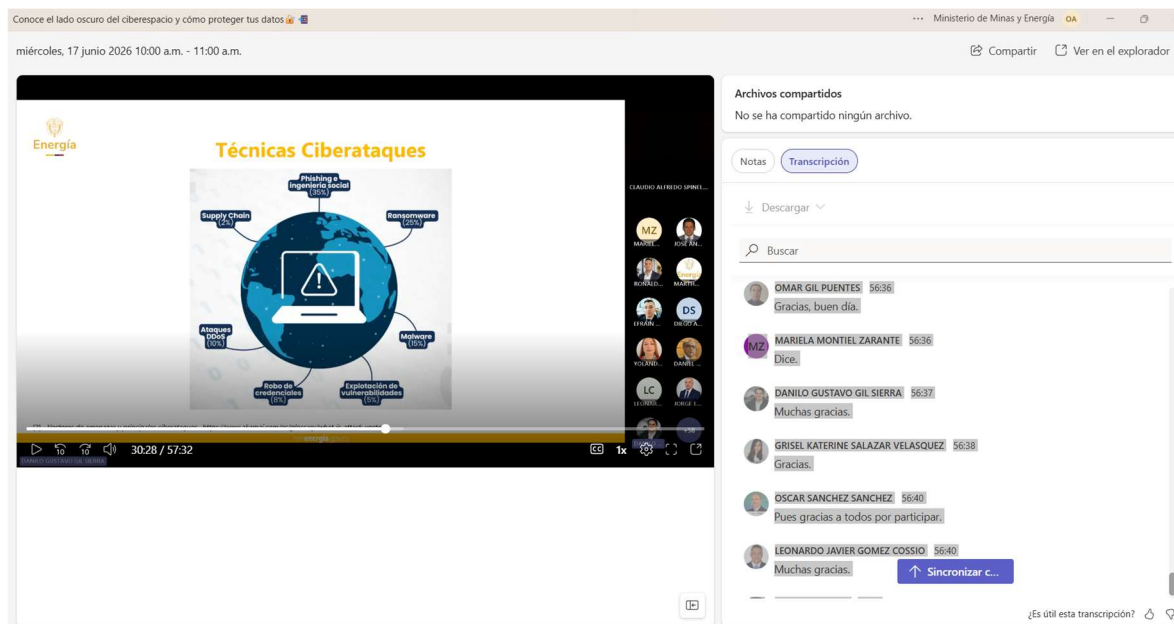
Posteriormente, el expositor presentó el concepto del ciberespacio como el quinto dominio estratégico, junto con los ámbitos terrestre, marítimo, aéreo y espacial, resaltando que en la actualidad gran parte de las actividades gubernamentales, económicas y sociales dependen del funcionamiento seguro de los sistemas digitales, razón por la cual la protección de la información se ha convertido en un componente esencial de la seguridad institucional.



Durante la capacitación se describieron las principales amenazas presentes en el entorno digital, incluyendo ataques de ingeniería social, campañas de *phishing*, robo de credenciales, programas maliciosos (*malware*), secuestro de información (*ransomware*), fraude informático y otras modalidades empleadas por actores maliciosos para obtener acceso no autorizado a sistemas o información sensible. Se enfatizó que muchas de estas amenazas no explotan únicamente vulnerabilidades tecnológicas, sino también errores humanos derivados del exceso de confianza, la falta de verificación de la información o el desconocimiento de las buenas prácticas de seguridad.

En este contexto, se insistió en la importancia de desarrollar una cultura de autoprotección digital, basada en hábitos seguros durante la navegación por Internet. Entre las principales recomendaciones se destacó la necesidad de verificar cuidadosamente la procedencia de los correos electrónicos antes de abrir enlaces o descargar archivos adjuntos; desconfiar de mensajes que soliciten información confidencial o credenciales de acceso; evitar ingresar datos institucionales en sitios cuya autenticidad no pueda ser comprobada; mantener actualizados los equipos,

sistemas operativos y programas de seguridad; utilizar conexiones seguras cuando se acceda a información institucional y reportar de manera inmediata cualquier comportamiento inusual de los equipos o posibles incidentes de seguridad.



Igualmente, se abordó el manejo seguro de las contraseñas, recomendando utilizar claves robustas, únicas para cada servicio y de difícil predicción, evitando compartirlas con terceros o reutilizarlas en diferentes plataformas. Durante el espacio de preguntas, el expositor manifestó que, aunque existen aplicaciones y servicios que generan automáticamente contraseñas complejas, considera más recomendable que cada usuario mantenga el control directo sobre sus credenciales y adopte mecanismos personales para administrarlas de manera segura, reduciendo la dependencia de servicios externos para su almacenamiento o generación.

Finalmente, se resaltó que la ciberseguridad constituye una responsabilidad compartida entre la entidad y cada uno de sus colaboradores, por lo que la prevención, la actualización permanente y la adopción de comportamientos responsables representan la principal barrera frente a las amenazas existentes en el ciberespacio. Como actividad de cierre, los participantes desarrollaron un ejercicio interactivo mediante la **plataforma Kahoot**, con el propósito de reforzar los conceptos expuestos y verificar la apropiación de los conocimientos adquiridos durante la capacitación.

Conoce el lado oscuro del ciberespacio y cómo proteger tus datos

miércoles, 17 junio 2026 10:00 a.m. - 11:00 a.m.

Ministerio de Minas y Energía

Archivos compartidos

No se ha compartido ningún archivo.

Notas Transcripción

Descargar

Buscar

OMAR GIL PUENTES 56:36
Gracias, buen día.

MARIELA MONTIEL ZARANTE 56:36
Dice.

DANILO GUSTAVO GIL SIERRA 56:37
Muchas gracias.

GRISSEL KATERINE SALAZAR VELASQUEZ 56:38
Gracias.

OSCAR SANCHEZ SANCHEZ 56:40
Pues gracias a todos por participar.

LEONARDO JAVIER GOMEZ COSSIO 56:40
Muchas gracias.

¿Es útil esta transcripción?

Principales temas abordados

- Concepto y características del ciberespacio.
- El ciberespacio como quinto dominio estratégico.
- Amenazas cibernéticas y delitos informáticos.
- Ingeniería social y técnicas de *phishing*.
- Riesgos asociados al uso de Internet y de los sistemas de información.
- Buenas prácticas para una navegación segura.
- Gestión segura de contraseñas y credenciales de acceso.
- Responsabilidad individual en la protección de la información institucional.
- Cultura de ciberseguridad y prevención de incidentes.
- Evaluación de conocimientos mediante actividad interactiva (Kahoot).

Compromisos

1. Implementar las buenas prácticas de ciberseguridad presentadas durante la capacitación en el desarrollo de las actividades laborales.
2. Fortalecer la protección de las credenciales de acceso y de la información institucional mediante el uso de contraseñas seguras y hábitos responsables de navegación.

3. Verificar la autenticidad de correos electrónicos, enlaces y sitios web antes de suministrar información o descargar archivos.
4. Reportar oportunamente a los canales institucionales cualquier incidente o sospecha de vulneración de la seguridad informática.
5. Contribuir al fortalecimiento de una cultura institucional de ciberseguridad basada en la prevención, la actualización permanente y el uso responsable de las tecnologías de la información.