

# ¡Bienvenidos al lanzamiento del Comité de Ciberseguridad - ACOLDC



**ACOLDC**  
Asociación Colombiana de DataCenter y Tecnología

**Este espacio nace para fortalecer la protección de las infraestructuras críticas digitales del país, consolidando capacidades, estándares y colaboración frente a un entorno de amenazas crecientes.**





# Agenda General

## Comité Ciberseguridad

- Bienvenida Oficial
- Propósito del comité & contexto sectorial (retos y mega tendencias Colombia).
- Postulaciones y votación por los miembros para la junta Directiva
- Presentación de la junta directiva, Nombre, cargo y responsabilidad
- Plan de trabajo.
- Priorización de 3–5 temas claves a trabajar (dot-voting) y definición de objetivos.
- Diseño de entregables: qué haremos, para quién y con qué evidencia.
- Gobernanza y calendario: líder, Co-líder, relator, dueños por entregable; fechas y modalidad.
- Acuerdos y próximos pasos.





# Comité de Ciberseguridad

## Propósito

Diseñar, articular y promover estándares, buenas prácticas y capacidades técnicas que protejan la infraestructura digital crítica frente a ciberamenazas, vulnerabilidades y riesgos operativos.

## Visión

Posicionar a Colombia como referente regional en ciberseguridad aplicada a centros de datos, integrando talento, regulación y tecnología bajo un enfoque preventivo, colaborativo y estratégico.



# Alcance



El Comité impulsará iniciativas en torno a:

- Estándares de protección para centros de datos e infraestructuras críticas.
- Protocolos de respuesta ante incidentes (IR) y continuidad de negocio (BCP).
- Prácticas de hardening digital.
- Evaluación de riesgos y marcos de gobernanza (NIST, ISO 27001, CSF).
- Articulación con CERTs, CSIRTs y entidades regulatorias.
- Concientización, cultura y formación especializada.





# Contexto y Retos del Sector

## Megatendencias

- Auge de ciberataques a infraestructuras críticas.
- Expansión de edge computing y entornos híbridos/multicloud.
- Integración de IA y automatización en defensa cibernética.
- Exigencias regulatorias en privacidad y protección de datos.

## Retos en Colombia

- Fragmentación en capacidades de detección y respuesta.
- Escasa adopción de marcos normativos globales.
- Baja inversión en seguridad OT y convergencia IT/OT.
- Déficit de talento certificado en ciberseguridad.
- Brechas en cultura organizacional sobre riesgos digitales.



# Postulaciones y votación para Junta Directiva del Comité



Invitamos a quienes deseen postularse para los roles de:

## ◆ **Director(a)**

Lidera el comité, coordina la planificación y ejecución de actividades, representa al grupo en los espacios institucionales y garantiza el cumplimiento de objetivos.

## ◆ **Co-Director(a)**

Apoya al director, lo reemplaza cuando es necesario y colabora activamente en la gestión y seguimiento de tareas del comité.

## ◆ **Relator(a)**

Lleva el registro de discusiones, acuerdos y avances, redacta las minutas de las reuniones y colabora en la sistematización de los entregables.

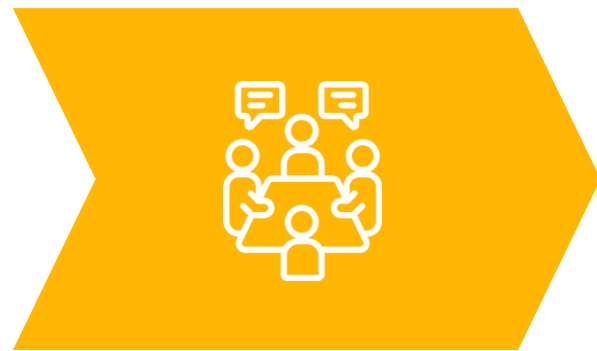
## ◆ **Secretario(a)**

Apoya la organización de reuniones, gestiona la comunicación interna del comité y mantiene actualizada la información de contacto y asistencia.

1. Invitamos a quienes deseen postularse o nominar a colegas a levantar la mano.
2. Posteriormente realizaremos la votación abierta entre los miembros presentes para definir el liderazgo del comité.

# Plan de Trabajo

## Reunión 1



1ra semana de diciembre  
(virtual)

## Reunión 2



3ra semana de enero  
(virtual)

## Reunión 3



3ra semana de febrero  
(virtual)

## Evento presencial



2da semana de marzo

## Seminario



OT/ICS Security

## Objetivo

Consolidar avances, validar entregables y compartir resultados con toda la comunidad ACOLDC.



# Líneas de acción

1. Elaborar documentos de referencia y buenas prácticas en ciberseguridad aplicadas a infraestructura crítica, alineados con marcos internacionales como NIST, ISO 27001, y CISA.
2. Diseñar protocolos unificados para la detección, respuesta y recuperación frente a ciberataques en centros de datos, integrando ejercicios de simulación (tabletop exercises) y planes de continuidad.
3. Promover la protección integral de los sistemas físicos y digitales, incluyendo BMS, DCIM y redes industriales, bajo modelos Zero Trust y segmentación segura.
4. Crear programas de capacitación, certificación y actualización técnica en ciberseguridad para operadores, ingenieros y personal de infraestructura digital.
5. Fomentar la colaboración público-privada y la conexión con CERTs nacionales e internacionales, para compartir alertas tempranas, amenazas emergentes y vulnerabilidades relevantes para el sector.
6. Desarrollar herramientas de diagnóstico y modelos de evaluación del nivel de madurez de ciberseguridad en data centers colombianos.
7. Impulsar campañas y eventos que fortalezcan la cultura organizacional de seguridad, desde la alta dirección hasta el personal operativo.



# Priorización de Temas Clave

Estos temas serán la base del plan de trabajo y deberán ser:

- Relevantes para el ecosistema
- Posibles de ejecutar en 90-120 días
- Generadores de impacto y evidencia

**Por cada tema seleccionado, definiremos:**

- Objetivo concreto
- A quién va dirigido (gobierno, industria, academia, integradores, operadores, etc.)
- Formato del entregable (guía, whitepaper, panel técnico, workshop, reporte, etc.)
- Evidencia y fuentes (indicadores, casos, normativas, benchmarks)

## **Gobernanza**

Dueños por entregable; fechas y modalidad.



# Acuerdos y Próximos Pasos



Finalmente, consolidaremos los acuerdos alcanzados hoy y dejaremos establecidos los próximos pasos inmediatos:

- Conformación oficial de los grupos de trabajo.
- Publicación del calendario de actividades.
- Apertura del canal de comunicación del comité.

El futuro térmico de nuestra infraestructura digital se construye hoy, ¡y ustedes son protagonistas!





**Proteger los datos es proteger el progreso. Y ese es el compromiso que hoy asumimos como gremio.**







# ¡GRACIAS!



**ACOLDC**

Asociación Colombiana de DataCenter y Tecnología