TÉRMINOS Y CONDICIONES
CYBERSECURITY AWARDS
ANDICOM 2026

En un mundo cada vez más digitalizado, la ciberseguridad se ha convertido en un aspecto fundamental para la protección de la información y los activos de las empresas. Con el objetivo de fomentar la cultura de la ciberseguridad en Colombia y reconocer a las organizaciones que implementan prácticas ejemplares, se crean los "**Cybersecurity Awards**".

Estos premios buscan incentivar la adopción de estrategias proactivas, la gestión eficaz de riesgos y la integración innovadora de la inteligencia artificial en materia de ciberseguridad. A través del reconocimiento de las mejores iniciativas, se pretende inspirar a otras empresas a fortalecer sus defensas digitales y contribuir a un ecosistema empresarial más resiliente ante las ciberamenazas.

A continuación, se detallan los términos y condiciones que regirán la participación en los "**Cybersecurity Awards**":

Este documento tiene como objetivo establecer las bases que regirán la participación en los "Cybersecurity Awards", incluyendo los requisitos de elegibilidad, el proceso de selección, los premios y las obligaciones de los participantes.

Es importante leer detenidamente estos términos y condiciones antes de presentar su candidatura. Al participar en los premios, se asume la aceptación total de los mismos.

1. CATEGORÍAS

La tercera edición del premio “Ciberseguridad Empresarial 2026” cuenta con cuatro categorías distintas, teniendo en cuenta las características y contextos de cada proyecto:

- **Premio a la Estrategia Proactiva de Ciberseguridad:** Reconoce a empresas que anticipan y previenen amenazas cibernéticas, fortaleciendo la resiliencia organizacional. Destaca proyectos que evalúan riesgos, implementan controles efectivos y toman decisiones informadas, mostrando un enfoque preventivo en ciberseguridad.

- **Premio al Mejor Proyecto de Gestión de Riesgos de Ciberseguridad:** Exalta los proyectos que demuestran un manejo exitoso de riesgos cibernéticos, destacando la efectividad de controles y decisiones dentro de un contexto empresarial.

Reconoce a empresas con estrategias integrales que protegen sistemas y datos, beneficiando a toda la organización.

- **Premio a la Integración de IA en Ciberseguridad:** Destaca a empresas que han incorporado inteligencia artificial en su ciberseguridad, mejorando la detección, prevención y respuesta a amenazas. Valora la innovación y la aplicación efectiva de IA para reforzar la seguridad y optimizar operaciones.

- **Excelencia en Educación y Cultura de Ciberseguridad:** La categoría destaca cómo el programa de capacitación en ciberseguridad de la organización ha abordado eficazmente los principales retos, proporcionando beneficios tangibles y mejoras en la postura de ciberseguridad.

2. CONDICIONES

Las empresas que deseen postular proyectos o iniciativas de ciberseguridad para los premios deberán cumplir con las siguientes condiciones:

- Las empresas deben estar registradas en Colombia
- Los proyectos deben haber sido implementados entre el 2025 y 2026
- Cada empresa pueda inscribir un (1) proyecto por cada categoría.
- Todos los proyectos deben incluir documentación detallada.
- Todos los proyectos deben contar con resultados medibles.
- En caso de que la información no esté detallada se solicitará una ampliación.
- Dependiendo de cada categoría los criterios de evaluación pueden tener un enfoque particular.

No se permitirá la postulación al concurso a las entidades representadas en los organizadores o evaluadores.

3. CRITERIOR DE EVALUACIÓN

Los criterios de evaluación se establecen por cada una de las categorías, los cuales serán los siguientes:

Categoría 1: Estrategia Proactiva de Ciberseguridad

1. Innovación
2. Anticipación a los Riesgos
3. Resiliencia Organizacional
4. Impacto
5. Documentación y Métricas

Categoría 2: Gestión de Riesgos de Ciberseguridad

1. Identificación de Riesgos
2. Efectividad de Controles
3. Toma de decisiones
4. Impacto
5. Documentación y Métricas

Categoría 3: Integración de IA en Ciberseguridad

1. Nivel de Integración
2. Capacidades Potenciadas
3. Innovación
4. Impacto
5. Escalabilidad

Categoría 4: Excelencia en Educación y Cultura de Ciberseguridad

1. Programas de Concienciación
2. Impacto Cultural
3. Iniciativas de Educación
4. Impacto en la organización

4. PROCESO DE EVALUACIÓN

La evaluación de los proyectos postulados por cada categoría se llevará a cabo mediante un proceso que se centrará en la validación del cumplimiento de cada uno de los criterios establecidos para las categorías. Este proceso será conducido por un comité de evaluación conformado por expertos de CINTEL y ETEK. Cada proyecto será evaluado en función de la información que sea proporcionada en los tiempos establecidos.

En caso de que se requiera ampliar la información que se proporcione por cada proyecto, los evaluadores realizarán la solicitud formal de ampliar la información requerida y en dado caso realizar una reunión virtual con el líder responsable del proyecto postulado.

El proceso de evaluación se da de la siguiente manera:

- Cada proyecto será evaluado con base en la documentación proporcionada por medio del formulario
- Primera revisión: La primera ronda de evaluación, implica un proceso de selección de las solicitudes recibidas. Los organizadores podrán solicitar cualquier aclaración o información adicional a los postulados, si es necesario.

- Segunda revisión: El Comité de Evaluación utilizando un sistema de puntuación determinará los semifinalistas, calificando cada postulación.
- Tercera revisión: La tercera ronda de evaluación será para discutir los materiales de solicitud de los semifinalistas, y finalizar la revisión de los semifinalistas para seleccionar a los finalistas.

Se solicitará a los finalistas un video descriptivo de la iniciativa ganadora, que no dure más de 2 minutos, para presentar en la ceremonia de premiación.

5. CRONOGRAMA

a. Apertura de postulaciones: 20 de abril de 2026
b. Difusión de la convocatoria: 20 de abril al 19 de junio de 2026
c. Recepción de las postulaciones: 20 de abril al 19 de junio de 2026
d. Cierre de postulaciones: 19 de junio de 2026
e. Análisis de postulaciones: 122 de junio al 24 de julio de 2026
f. Información Complementaria: 22 de junio al 24 de julio de 2026
g. Análisis de finalistas y recepción de videos: 27 a 31 de julio de 2026
h. Anuncio de finalistas: 31 de julio de 2026
i. Elaboración de placas/trofeos: 3 a 31 de agosto de 2026
j. Ceremonia entrega de premios en el marco del congreso ANDICOM: 02 de septiembre de 2026
k. Agradecimientos: 07 al 11 de septiembre de 2026

6. PROCESO DE REGISTRO

Las empresas que deseen postular sus proyectos e iniciativas deberán diligenciar el formulario que se encuentra en el siguiente link: https://forms.cloud.microsoft/r/CaQBYi0k3E?origin=lprLink

7. PREMIOS

Los finalistas serán invitados a la ceremonia en ANDICOM 2026, en Cartagena, Colombia donde serán anunciados los ganadores y entregados los premios **Cybersecurity Awards 2026**. Esta invitación incluye únicamente el ingreso al Congreso ANDICOM 2026, incluido los eventos relacionados con el precongreso. Se entregará una placa/trofeo de reconocimiento a aquellos proyectos que sean escogidos como ganadores en cada categoría.

La invitación no incluye viáticos, traslados (aéreos o terrestres), alojamiento, ni otros gastos en los que pueda incurrir el ganador del concurso.

8. CEREMONIA

La ceremonia de premiación se llevará a cabo el 02 de Septiembre de 2026 en el marco del Congreso ANDICOM.

Los ganadores del primer lugar de cada categoría podrán asistir a la Ceremonia celebrada en Cartagena, Colombia. La ceremonia constará de los siguientes componentes:

- Presentación de las iniciativas ganadoras **Cybersecurity Awards -** ANDICOM 2026.
- Ceremonia de entrega de premios que destaca a los Ganadores del Premio en cada categoría.

9. REGULACIONES

El solicitante es totalmente responsable de redactar y enviar la información de la solicitud y todos los materiales de respaldo. El solicitante es el único responsable de cualquier violación de derechos de propiedad intelectual, derechos de propiedad industrial, derechos de autor y/o derechos de imagen y deberá asumir total responsabilidad respecto de cualquier asunto de terceros. Los organizadores del **Cybersecurity Awards** no son responsables de ninguna infracción o información errónea proporcionada por los solicitantes.

Los textos completos o resúmenes de todas las solicitudes y materiales de apoyo presentados a los **Cybersecurity Awards** se pueden publicar en el sitio web oficial de CINTEL, y cualquier otro recurso en línea y/o cualquier publicación. La solicitud al **Cybersecurity Awards** implica el consentimiento a estos términos y condiciones.

Se solicitará a los ganadores que envíen un vídeo que presente el proyecto postulado para la Ceremonia del **Cybersecurity Awards** en ANDICOM 2026.

Cualquier información que el solicitante considere sensible o confidencial y, por lo tanto, no desee que los organizadores del **Cybersecurity Awards** hagan pública, debe notificarse con antelación por escrito a los siguientes correos electrónicos adiaz@cintel.org.co y jcorrea@etek.com al presentar la solicitud.

Disposiciones Generales:

- Las decisiones del jurado son definitivas y no se pueden impugnar.
- Los proyectos y empresas ganadoras pueden ser objeto de promoción en medios de comunicación y eventos de CINTEL y ETEK.

- Los organizadores del concurso garantizarán la confidencialidad de la información proporcionada por las empresas participantes y solo la utilizarán con fines de evaluación y selección de los ganadores.
- Los organizadores del concurso se reservan el derecho de realizar modificaciones en estos términos y condiciones en cualquier momento, previa notificación a todas las partes involucradas.

Autorización de tratamiento de datos personales

Al realizar la postulación de la iniciativa al **Cybersecurity Awards** el organizador entiende que el participante ha leído, conoce y acepta en su integridad:

1. Política de Tratamiento de datos personales de CINTEL, ubicada en el siguiente link https://cintel.co/wp-content/uploads/2021/02/Politica-de-tratamiento-de-datos-personales-CINTEL.pdf

2. Autorización para el Tratamiento de datos personales. Con la aceptación y envío del formulario autoriza a CINTEL para el tratamiento de sus datos personales de conformidad con la autorización ubicada en el siguiente link https://cintel.co/autorizacion-tratamiento-datos-personales/

3. Política Protección de Datos Personales de ETEK, ubicada en el siguiente link https://etek.com/es/politica-proteccion-datos-personales/

10. PREGUNTAS

Para consultas o más detalles, comuníquese a los siguientes correos electrónicos: adiaz@cintel.org.co y jcorrea@etek.com