Centro de Ciberseguridad Industrial

# CONCURSO

## ARQUITECTURA SEGURA DE TECNOLOGÍAS INDUSTRIALES 2022

## BASES DEL CONCURSO

**ANTECEDENTES DEL CONCURSO**

1. El CENTRO DE CIBERSEGURIDAD INDUSTRIAL es una organización sin ánimo de lucro que tiene como propósito proporcionar un espacio para profesionales y entidades -públicas y privadas- donde colaborar para mejorar el nivel de Ciberseguridad en la industria.

2. La ciberseguridad industrial identifica riesgos tecnológicos y propone su gestión para reducir las consecuencias de este riesgo en entornos industriales.

3. Dentro de este marco el Centro de Ciberseguridad Industrial convoca el "Concurso Arquitectura Segura de Tecnologías Industriales 2022 "(en adelante, "EL CONCURSO"). EL CONCURSO tiene como finalidad motivar e incentivar el aprendizaje premiando al profesional o al estudiante por sus conocimiento y habilidades para mejorar la seguridad y reducir el riesgo de las tecnologías industriales.

**BASES DEL CONCURSO**

4. Para intervenir en EL CONCURSO, cada PARTICIPANTE deberá acreditar ser miembro del ecosistema del Centro de Ciberseguridad Industrial, es decir, tener una cuenta en la **plataforma de conocimiento,** podrá acceder en el siguiente enlace: Concurso. Si no dispone todavía de una cuenta puede registrarse como miembro básico en el siguiente enlace: Registro

Una vez registrado en la plataforma de conocimiento podrá inscribirse accediendo al enlace: Inscripción

El solicitante admitido para participar en el concurso dispondrá de acceso a la **plataforma RECIN,** podrá acceder en el siguiente enlace: https://recin.cci-es.org/ para realizar dos (2) proyectos mediante la cuenta de la **plataforma de conocimiento**.

5. El CONCURSO consiste en desarrollar y presentar tres (3) entregables, dos de ellos serán arquitecturas creadas utilizando la plataforma RECIN (la cual cuenta con una plantilla para crear arquitecturas tecnológicas)

- una **arquitectura inicial** de un posible escenario industrial funcional donde no se ha contemplado en su diseño la seguridad tecnológica, como el siguiente **ejemplo**, presentando un documento en formato pdf donde podrá poner los antecedentes o explicaciones que considere necesarios sobre la infraestructura.

- una **arquitectura final** que será desarrollada a partir de la anterior arquitectura inicial pero donde si se contemple la seguridad tecnológica como en el siguiente **ejemplo**, utilizando para ello la plataforma RECIN https://recin.cci-es.org/ y completando la información de zonas, conductos y componentes para para presentar un informe en formato pdf con los requisitos de ciberseguridad necesarios que genera la plataforma.

- un documento en pdf que deberá incluir las soluciones y/o servicios propuestos para cubrir cada uno de los requisitos de los componentes de cada zona y conducto de la **arquitectura final** utilizando para ello el catálogo activo del Centro de Ciberseguridad Industrial https://catalogo.cci-es.org/requisitos-iec62443/?reqId=9 al que podrá conectarse con la cuenta de miembro.

A la suma de estos tres entregables se les denominará, en adelante, "LA PROPUESTA".

6. LA PROPUESTA de EL PARTICIPANTE deberá demostrar conocimiento y cierto nivel de iniciativa.

7. A la hora de participar deberá indicarse el sector industrial al que pertenece la arquitectura segura que se presentará, agua, eléctrico, transporte, alimentación, químico, salud, fabricación u otros sectores a elección de EL PARTICIPANTE.

Centro de Ciberseguridad Industrial

## PARTICIPANTES Y CATEGORÍAS

8. Pueden participar profesionales de cualquier ámbito y estudiantes de un grado universitario o de formación profesional.

Cada PROPUESTA será presentada por un participante individual o por un equipo conformado (en este último caso) hasta por un máximo de tres (3) participantes de una empresa o centro académico. Al participante individual o al equipo nos referimos en este acuerdo bajo la denominación (en singular) de "EL PARTICIPANTE".

9. LA PROPUESTA a presentar **NO DEBE**:

A. Ser copia o réplica de alguna arquitectura existente.
B. Contener información confidencial o sensible de ninguna empresa u organización.
C. Ser de carácter bélico o violento.
D. Fomentar la violencia física o psicológica.
E. Emplear palabras, sonidos o imágenes ofensivas u obscenas.

10. EL PARTICIPANTE, si es estudiante, podrá ser apoyado por un profesor que cumpla el rol de mentor del programa academia https://www.cci-es.org/ecosistema/programa-academia/ . El profesor deberá ser docente en el centro de EL PARTICIPANTE.

11. EL PARTICIPANTE podrá buscar asesoría y ayuda para el desarrollo de LA PROPUESTA, pero las ideas, el trabajo y su concreción en el diagrama de la arquitectura y descripción deben ser de EL PARTICIPANTE. Está prohibido que un miembro del equipo de expertos del Centro de Ciberseguridad Industrial brinde asesoría a la presentación de LA PROPUESTA.

## DINÁMICA DEL CONCURSO

12. EL PARTICIPANTE deberá primero solicitar participar en el concurso a través del enlace: Inscripción en la plataforma de conocimiento https://conocimiento.cci-es.org/en el apartado correspondiente al concurso.

13. EL PARTICIPANTE elaborará LA PROPUESTA que una vez finalizada, deberá subir en la plataforma de conocimiento https://conocimiento.cci-es.org/ en el apartado correspondiente al concurso a través del enlace designado para ello deberá cargar los tres entregables mencionados en el enlace Sube tus entregables en: concurso.

14. El Centro de Ciberseguridad Industrial notificará la recepción de los entregables a EL PARTICIPANTE.

15. El Centro de Ciberseguridad Industrial podrá solicitar a EL PARTICIPANTE que complete la información faltante o que aclare inconsistencias.

16. El Centro de Ciberseguridad Industrial evaluará las propuestas recibidas, definirá los ganadores del concurso comunicará los resultados.

## EVALUACIÓN DE LAS PROPUESTAS

17. Todas las propuestas serán analizadas por un jurado integrado por expertos del Centro de Ciberseguridad Industrial relacionados con los campos de conocimiento objeto del concurso. La identidad de los miembros del jurado se hará pública oportunamente en la web de CCI.

18. Los miembros del jurado calificarán cada PROPUESTA de manera aislada y sin conocimiento de la identidad de EL PARTICIPANTE. Los criterios y pesos de evaluación son los siguientes:

- **Descripción del contexto de la arquitectura y sus riesgos** 10
- **Claridad de los diagramas de arquitecturas presentados** 10
- **Originalidad de la arquitectura segura final** 10
- **Grado en que se reduce el riesgo tecnológico** 10

Puntuación total 40

19. Cada miembro del jurado calificará LA PROPUESTA en una escala del 0 al 10, de acuerdo con los criterios de evaluación indicados. El puntaje de cada PROPUESTA será el promedio de las calificaciones de los miembros del jurado.

20. Los tres concursantes con mejor puntuación ocuparán primer, segundo y tercer puesto según corresponda. En el caso de que se produzca empate, el equipo directivo del Centro de Ciberseguridad Industrial determinará el orden de los concursantes ganadores.

21. Las evaluaciones del jurado serán inobjetables, y contra ellas no procederá recurso impugnatorio alguno. Las evaluaciones individuales de cada jurado sobre cada propuesta no será información pública.

## COMUNICACIÓN DE RESULTADOS

22. Los resultados de la evaluación del jurado se publicarán en el sitio web del concurso y en las redes sociales o medios de comunicación del Centro de Ciberseguridad Industrial, además de notificar a los participantes vía correo electrónico.

23. Las tres propuestas ganadoras serán publicadas en la web del Centro de Ciberseguridad Industrial con la correspondiente información de la autoría de los ganadores.

## PREMIOS Y RECONOCIMIENTOS

24. Los premios y reconocimientos del presente concurso serán:

- **Para los 3 ganadores:**
  - Publicación de sus arquitecturas en la web y medios de comunicación del Centro de Ciberseguridad Industrial.
  - Diploma de ganador indicando el puesto obtenido.
  - Un trofeo de reconocimiento.
  - El concursante individual o los miembros del equipo que obtenga el primer puesto obtiene una plaza en el máster profesional de ciberseguridad industrial y una plaza en un taller de la Escuela del Centro de Ciberseguridad Industrial.
  - El concursante individual o los miembros del equipo que obtenga el segundo puesto obtiene una plaza en el curso multidisciplinar de ciberseguridad industrial y una plaza en un taller de la Escuela del Centro de Ciberseguridad Industrial.
  - El concursante individual o los miembros del equipo que obtenga el tercer puesto obtienen una plaza en el curso de responsable de ciberseguridad en IACS y una plaza en un taller de la Escuela del Centro de Ciberseguridad Industrial.
- **Para los profesores mentores de cada participante ganador:**
  - Diploma de participación.
  - Reconocimiento en la publicación de las arquitecturas.
- **Para los 10 finalistas no ganadores:**
  - Diploma de finalista.
- **Para los profesores mentores de los 10 finalistas no ganadores:**
  - Diploma de participación.

## CRONOGRAMA GENERAL DEL CONCURSO

25. El cronograma general del concurso será:

| EVENTO | FECHA |
|---|---|
| Inscripción | Del 28 de febrero al 30 de marzo |
| Webinar Aplicando RECIN | 9 de marzo |
| Cierre de recepción de arquitecturas | 20 de abril |
| Evaluación del Jurado | 20 de abril al 5 de mayo |
| Publicación de Ganadores | 5 de septiembre |
| Entrega de premios | 27 de septiembre (Congreso Internacional CCI) |

Centro de
Ciberseguridad Industrial

## Términos y condiciones adicionales del CONCURSO

1. La participación en EL CONCURSO implica la aceptación total de sus bases, términos y condiciones. Los alumnos participantes, en tanto menores de edad, son representados en este acuerdo por sus padres, tutores o representantes legales, quienes declaran conocer y aceptar íntegramente lo establecido en las bases.
2. EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL presume que los datos consignados por EL PARTICIPANTE son verdaderos, exactos y, por consiguiente, fidedignos. Sin perjuicio de ello, se reserva el derecho de confirmar la veracidad de estos. Cuando de la evaluación realizada se desprenda que la información presentada, en todo o en parte, es falsa o inexacta, EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL podrá resolver unilateralmente cualquier acuerdo y eliminar al participante de EL CONCURSO. Si la información fuese incompleta o inconsistente, podrá darle a EL PARTICIPANTE la opción de subsanar los defectos encontrados.
3. EL PARTICIPANTE no podrá ceder a terceros ni sus derechos ni la posición que ostenta en EL CONCURSO y/o en el Registro de Participación.
4. EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL reconoce los derechos morales de EL PARTICIPANTE en las obras o diseños industriales. En consecuencia, colocará sus créditos y hará público reconocimiento a su trabajo en la muestra o exposición, en la web, brochure o donde corresponda.
5. EL PARTICIPANTE otorga una cesión de derechos a favor de EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL respecto del diagrama de arquitectura, información facilitada, cesión de derechos no exclusiva, de alcance mundial, gratuita y perpetua, para que EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL pueda usarlos de forma conjunta o por separado, pudiendo reproducirlos, distribuirlos, comunicarlos públicamente y transformarlos, teniendo EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL el derecho a hacer o producir obras derivadas de los mismos, exponerlos y colocarlos en la web, todo ello dentro del marco de las actividades de EL CONCURSO, en material publicitario del mismo, en la difusión o promoción de actividades efectuadas por EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL y en usos similares.
6. EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL no estará obligado a devolver la documentación, obras o diseños que EL PARTICIPANTE entregue a EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL en razón de EL CONCURSO.
7. En el marco de EL CONCURSO y de las actividades de difusión y promoción del mismo, EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL podrá hacer uso respetuoso de la imagen, nombre y voz de EL PARTICIPANTE y, si hubiese, del mentor; así como del título, nombre y/o denominación de LA PROPUESTA.
8. EL PARTICIPANTE, sus padres, tutores o representantes reconocen y aceptan que en el ámbito de EL CONCURSO entregarán cierta información personal que EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL utilizará únicamente para los fines y actividades del mismo, en consonancia con las normas legales sobre la materia. Aceptan asimismo recibir correos electrónicos con información sobre las actividades académicas de EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL, los que no serán considerados spam.
9. EL CONCURSO se rige enunciativamente por las condiciones aquí establecidas. EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL se reserva el derecho de dictar disposiciones adicionales aplicables al mismo. En caso de duda o ambigüedad sobre los alcances, términos y condiciones, EL PARTICIPANTE manifiesta su expresa voluntad de someterse a la interpretación que efectúe EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL. Las decisiones de EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL no serán materia de revisión, reconsideración ni apelación.
10. EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL podrá resolver cualquier acuerdo si EL PARTICIPANTE, sus padres, tutores o representantes legales incumplen las obligaciones establecidas en el mismo, en especial aquellas relacionadas con la inscripción y el cumplimiento de sus requisitos.
11. EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL no se responsabilizará en caso de que algún PARTICIPANTE haya copiado, plagiado o reproducido una obra, texto o imágenes de terceros, sin autorización de éstos. Si EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL detectase plagio o copia sustancialmente similar en LA PROPUESTA; si faltase el consentimiento válido por parte de EL PARTICIPANTE y/o sus padres, tutores o representantes legales, podrá a su sola discreción separar de inmediato a EL PARTICIPANTE infractor. Hará su mejor esfuerzo por corregir la situación, según el momento y circunstancias. EL PARTICIPANTE y/o sus padres, tutores o representantes legales podrán ser solidariamente responsables de los daños y perjuicios que ocasionasen a EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL por su conducta infractora, en particular por cualquier repercusión negativa en su reputación como entidad universitaria.
12. Si alguno de los numerales o cláusulas de las bases del concurso fuese total o parcialmente nulo o se anulase, el resto no quedará sin efecto, sino que conservará plena validez y total eficacia.

**Organiza:**

**EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL**

**Para mayor información, contactarse con:**
EL CENTRO DE CIBERSEGURIDAD INDUSTRIAL
Teléfono: +34 910 910 751

E-mail: info@cci-es.org