CENTRO DE CIBERSEGURIDAD INDUSTRIAL

EDICIÓN 2022

RECIN

MANUAL DE USO

PATRONES DE NIVELES DE SEGURIDAD IEC-62443

Centro de Ciberseguridad Industrial

El **Centro de Ciberseguridad Industrial** (CCI) es una organización independiente, sin ánimo de lucro, cuya misión es impulsar y contribuir a la mejora de la Ciberseguridad Industrial, en un contexto en el que las organizaciones de sectores como el de fabricación o el energético juegan un papel crítico en la construcción de la sociedad actual, como puntales del estado del bienestar.

El CCI afronta ese reto mediante el desarrollo de actividades de investigación y análisis, generación de opinión, elaboración y publicación de estudios y herramientas, e intercambio de información y conocimiento, sobre la influencia, tanto de las tecnologías, incluidos sus procesos y prácticas, como de los individuos, en lo relativo a los riesgos -y su gestión- derivados de la integración de los procesos e infraestructuras industriales en el Ciberespacio.

CCI es, hoy, el ecosistema y el punto de encuentro de las entidades -privadas y públicas- y de los profesionales afectados, preocupados u ocupados de la Ciberseguridad Industrial; y es, asimismo, la referencia hispanohablante para el intercambio de experiencias y la dinamización de los sectores involucrados en este ámbito.

Paseo de las Delicias, 30, 2ª Planta

28045 MADRID

Tel.: +34 910 910 751

e-mail: info@cci-es.org

www.cci-es.org

Blog: blog.cci-es.org

Twitter: @info_cci

LinkedIn: www.linkedin.com/in/centrociberseguridadindustrial

Índice

Introducción

RECIN es una plataforma ágil para facilitar la incorporación de requisitos de ciberseguridad en proyectos industriales, tanto de automatización, como de digitalización. Está basada en el estándar IEC-62443-3-3 y permite definir la arquitectura básica de un proyecto mediante zonas y conductos, así como generar los requisitos de ciberseguridad de forma automática basándose en la criticidad de integridad, disponibilidad y confidencialidad que puedes establecer para cada componente de las zonas y conductos del proyecto.

Para acceder a la plataforma RECIN necesita primero estar registrado como miembro de CCI, podrá utilizar el mismo usuario y contraseña que utiliza en la plataforma colaborativa de CCI: https://www.cci-es.org/colaborativa Acceso a RECIN mediante enlace: https://recin.cci-es.org/

Con esta plataforma podrá crear proyectos desde cero o crear plantillas que podrán utilizarse como base para tus nuevos proyectos, para ello simplemente debes crear un proyecto y copiarlo tantas veces como lo necesites usando

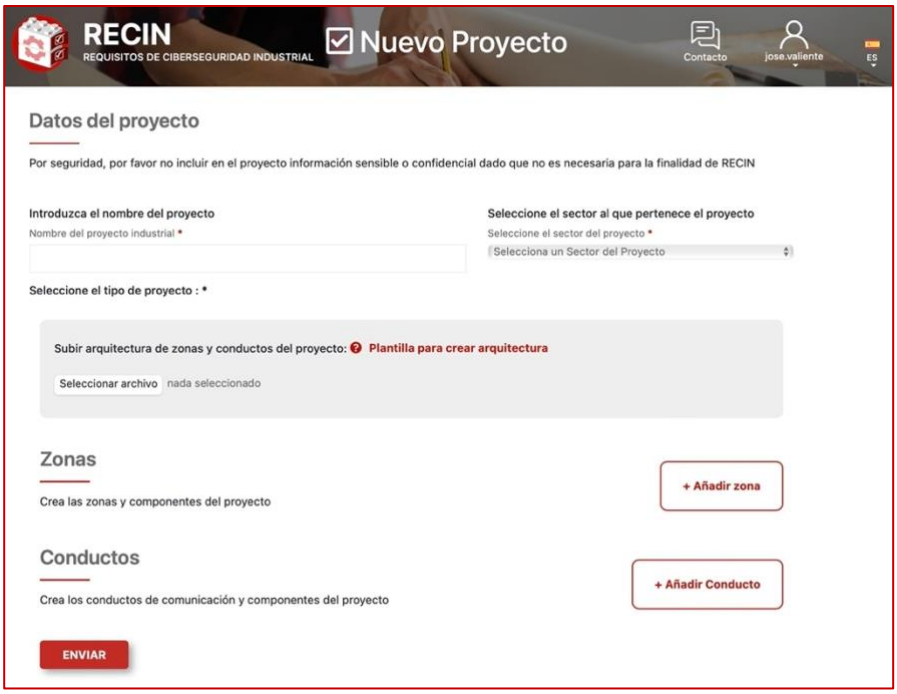
La plataforma incorpora un buscador Buscar: que te facilitará la localización de los proyectos para poder editarlos mediante , también podrá generar un informe del proyecto con los requisitos de ciberseguridad mediante

Desde la pantalla principal podrá borrar proyectos en cualquier momento mediante .

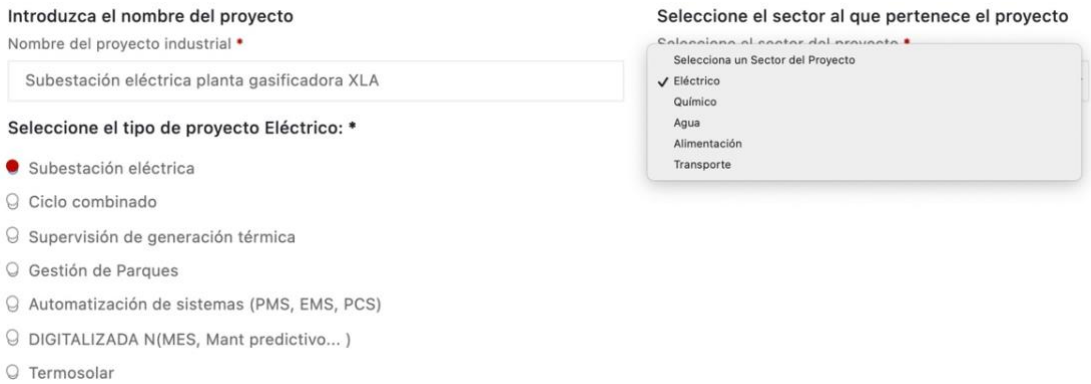
También podrá consultar un histórico de las acciones Crear, Editar, Clonar y Eliminar proyectos pulsando sobre HISTÓRICO y accederá a:

Creación de proyecto

Para crear un proyecto deberá usar CREAR NUEVO PROYECTO y accederá al siguiente formulario:

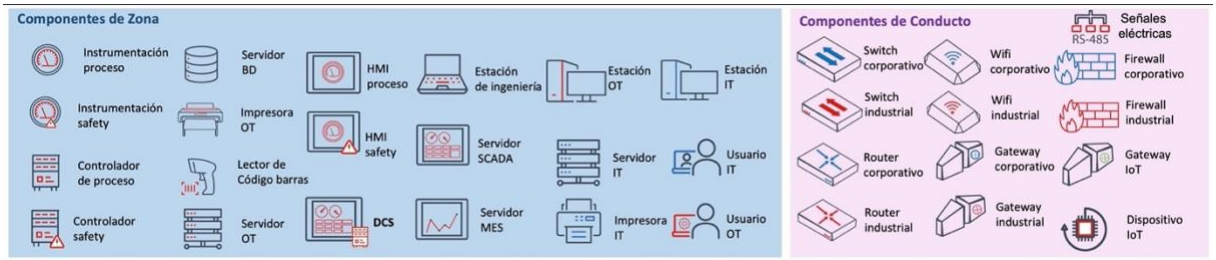


Donde deberá indicar el nombre al proyecto. Si quieres crear una plantilla, le recomendamos que el nombre del proyecto empiece por “Plantilla – XXX” lo cual te facilitará la búsqueda de plantillas. Una vez indicado el nombre, deberá seleccionar el sector al que pertenece su proyecto. Si no apareciese el sector de su proyecto, deberá enviar un email a recin@cci-es.org para indicar su sector y los tipos de proyectos que necesita, puedes ver tipos de proyectos de otros sectores. En menos de 24 horas daremos de alta tu sector y los tipos de proyectos, avisándote por email de su incorporación.

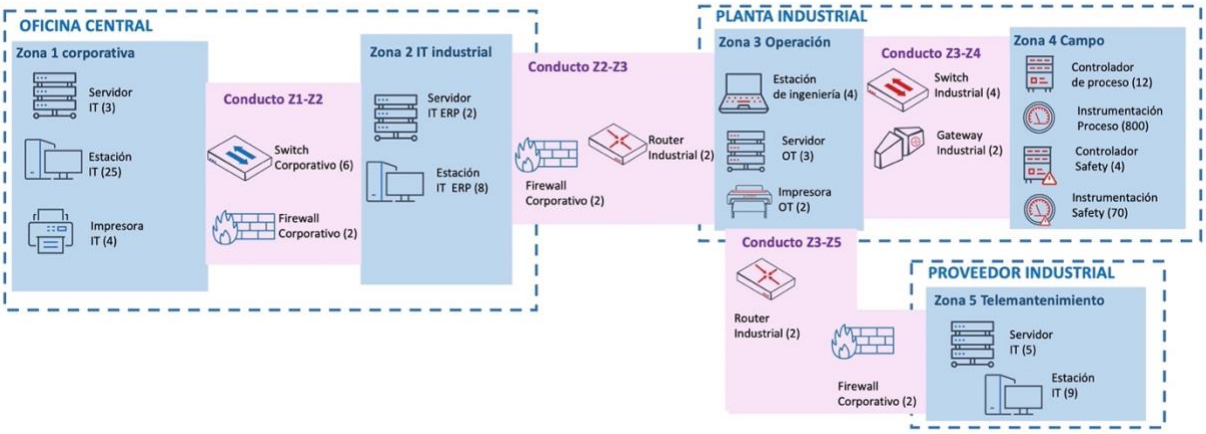


Una vez haya introducido el nombre del proyecto, su sector y el tipo deberá crear una arquitectura básica que incluya zonas y conductos de su proyecto y todos los tipos de componentes para ello dispones de una plantilla en ppt.

Podrá descargar la plantilla desde **Plantilla para crear arquitectura** donde encontrará todos los componentes y ejemplo para preparar la arquitectura de su proyecto:



Ejemplo:



Una vez haya creado la arquitectura deberá guardarla como un fichero con formato de **imagen jpg** y subir el archivo mediante la opción **Seleccionar archivo**.

La arquitectura deberá agrupar todos los componentes en zonas y conductos. Una **Zona** es una agrupación lógica o física de activos industriales, componentes de tipo sistema, los cuales deben compartir los mismos requisitos de seguridad. Un **Conducto** es un tipo particular de zona que agrupa componentes de comunicaciones que permiten transmitir datos o información entre diferentes zonas.

Algunas recomendaciones a la hora de crear la arquitectura de tu proyecto según el estándar IEC-62443:

- Los componentes de sistemas de información (TI) y los componentes de sistemas de control industrial (OT) deben estar agrupados en zonas separadas porque la responsabilidad de estos recae en diferentes áreas de las organizaciones, determinado por los resultados de análisis de riesgos previos, y habitualmente su ubicación es diferente. Es importante entender que la principal diferencia entre ambos entornos es que los sistemas de control industrial tienen impacto directo en la

salud de las personas y el medio ambiente, además de que pueden afectar a la producción y a la imagen corporativa cuando se produce un incidente.

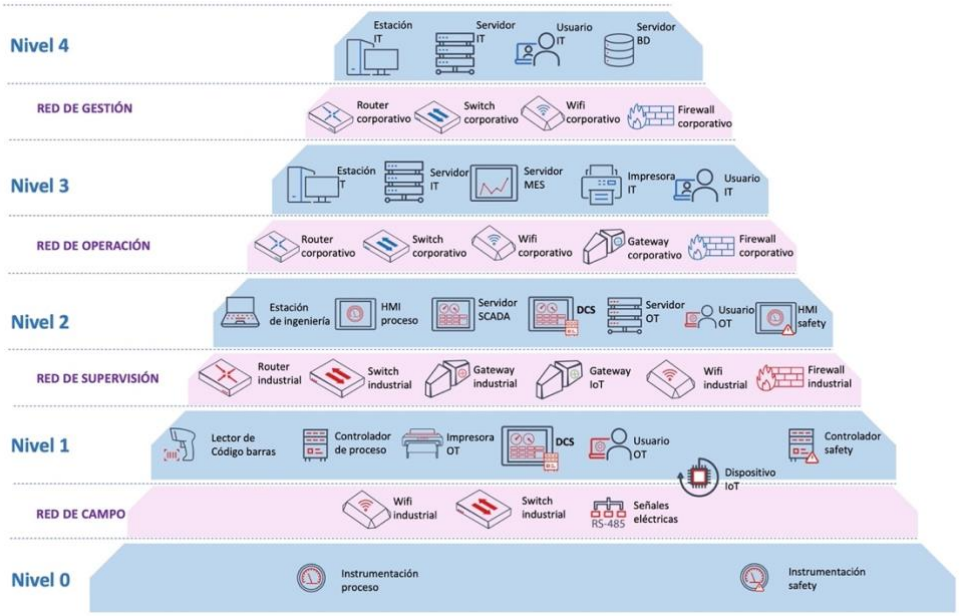
- Los activos identificados como Sistemas Instrumentados de Seguridad (SIS) deben estar en Zonas distintas. Los SIS por su naturaleza poseen requisitos de seguridad diferentes a los demás componentes de un sistema de control industrial.

- Los activos o dispositivos que se conectan temporalmente deben ser separados en Zonas distintas. Dispositivos como portátil de mantenimiento, dispositivos de análisis de ciberseguridad portátiles (herramientas de análisis de comportamiento en función de captura de trafico de red), dispositivos de almacenamiento USB, entre otros, suelen estar expuestos a un número mucho mayor de amenazas que aquellos que se encuentran permanentemente dentro de una zona. Es por ello que estos dispositivos deben ser modelados en una zona separada. La principal razón es que al ser dispositivos de conexión temporal es muy probable que también se conecten a otras redes fuera de la zona cuyos requisitos de ciberseguridad no cumplan los establecidos para ella.

- Las comunicaciones inalámbricas deben ubicarse en una o más zonas separadas de las comunicaciones cableadas. Las comunicaciones inalámbricas no son controladas por muros o gabinetes y por lo tanto poseen un mayor nivel de exposición que las comunicaciones cableadas.

Alta de zonas y sus componentes

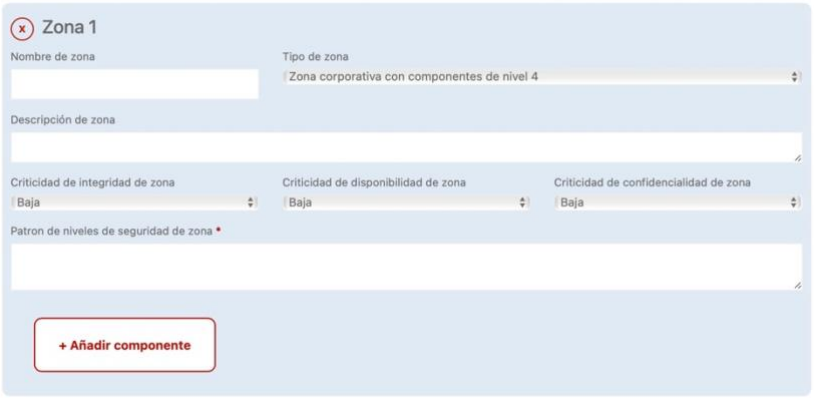
Dentro del proyecto dará de alta las zonas y sus componentes según la arquitectura definida, para ello deberá indicar un nombre de zona y seleccionar un tipo de zona, los tipos de zonas corresponder a uno o varios niveles de la pirámide purdue que puedes ver representada a continuación:



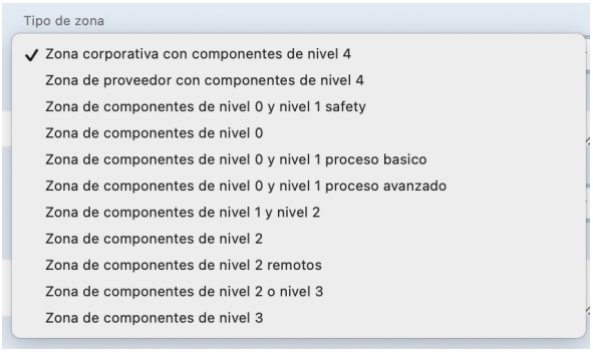
Como puede observar en la imagen anterior en el **nivel 0** se encuentran los componentes de tipo instrumentación de sensores y actuadores, tanto para proceso, como para instrumentación. En el **nivel 1** se encuentran los componentes de control, como los controladores de proceso o safety, como PLCs o RTUs, impresora OT o lectores de código de barras, así como DCS (la capa de control de un sistema de control distribuido). En el **nivel 2** se encuentran los componentes de supervisión, como HMI, servidor SCADA, o la capa de supervisión de un DC. En el **nivel 3** encontramos componentes de operación o de optimización para mantenimiento predictivo, por ejemplo, como servidor MES u otro tipo de servidores IT o estaciones. Finalmente, en el **nivel 4** se encuentran los componentes de sistemas de información.

Para añadir una zona dispone del botón 

que desplegará el siguiente formulario:



Deberá seleccionar el tipo de zona que corresponda seleccionando uno de los 11 tipos que existen:



La selección del tipo de zona indicará el tipo de componentes que tendremos. A continuación, debers indicar la criticidad en cuanto a la perdida de integridad, disponibilidad y confidencialidad que tiene la zona, es decir el impacto que supondría la perdida de integridad, disponibilidad y confidencialidad. La criticidad en estas tres dimensiones se expresará de forma cualitativa en 4 grados (Baja, Media, Alta y Muy Alta):

Para establecer el grado de criticidad de perdida de cada una de las dimensiones debería realizarse un análisis de impacto que determine la valoración en base a las consecuencias que tendría la perdida de integridad, disponibilidad y confidencialidad de la zona, utilizando una tabla de criterios de valoración, por ejemplo, con criterios de perdida de producción, coste de recuperación, perdida de vidas, perdida de imagen, impacto ambiental y de seguridad operacional.

Si no fuera posible realizar este análisis de riesgos le facilitamos una tabla orientativa para cada tipo de zona y sector, se ha elaborado en base al criterio de profesionales del sector:

	SECTORES														
TIPO DE ZONAS	Agua			Químico			Alimentación			Transporte			Eléctrico		
Zona corporativa con componentes de nivel 4	M	M	A	A	M	A	A	M	A	A	M	B	A	M	A
Zona de proveedor con componentes de nivel 4	A	MA	A	A	B	A	A	B	M	M	B	M	A	A	A
Zona de componentes de nivel 0 y nivel 1 safety	MA	MA	B	MA	MA	M	MA	MA	M	MA	MA	B	MA	MA	B
Zona de componentes de nivel 0	MA	MA	B	B	B	B	B	B	B	B	B	B	MA	MA	B
Zona de componentes de nivel 0 y nivel 1 proceso basico	MA	MA	B	A	M	B	A	M	B	A	A	B	MA	MA	B
Zona de componentes de nivel 0 y nivel 1 proceso avanzado	MA	MA	B	A	M	A	A	M	M	A	A	M	MA	MA	B
Zona de componentes de nivel 1 y nivel 2	MA	MA	M	MA	M	A	A	M	A	A	A	M	MA	MA	M
Zona de componentes de nivel 2	MA	M	M	MA	M	A	A	M	A	A	M	B	MA	A	M
Zona de componentes de nivel 2 remotos	MA	A	M	M	M	A	M	M	A	A	M	B	MA	A	M
Zona de componentes de nivel 2 o nivel 3	MA	A	M	A	M	A	A	M	A	A	B	A	A	A	M
Zona de componentes de nivel 3	MA	M	A	A	B	A	A	B	A	A	B	A	A	M	M
	I	D	C	I	D	C	I	D	C	I	D	C	I	D	C

I	Integridad
D	Disponibilidad
C	Confidencialidad

MA	Muy Alta
A	Alta
M	Media
B	Baja

Para elaborar la tabla se ha seguido la siguiente matriz de valoración de impacto:

Valoración	Impacto operativo	Impacto Medioambiente o salud	Impacto legal	Impacto patrimonial	Impacto reputacional
Muy Alta	+24 h paro	Perdida vidas o impacto ambiental alto	Sanción fuerte	Más 50% beneficio	En clientes importantes
Alta	+8 h paro	Lesiones altas o impacto ambiental medio	Sanción cambios	25% al 50% beneficio	En clientes medios y proveedores
Media	+4 h paro	Lesiones medias o impacto ambiental bajo	Sanción tiempo	1% al 25% beneficio	En proveedores
Baja	Menor de 1 h paro	Sin lesión Sin impacto	Gestión adminis	Menor 1% beneficio	Puntual y sin impacto importante

Una vez establecida la criticidad de cada una de las dimensiones se genera automáticamente un patrón de seguridad que establece los niveles de seguridad para cada una de las 7

categorías de IEC-62443 según la correspondencia de criticidad definida por CCI y que puedes ver en la siguiente tabla:

Patrones de seguridad (Correspondencia de criticidad con categorías de seguridad IEC-62243)

PATRON	INTEGRIDAD	DISPONIBILIDAD	CONFIDENCIALIDAD	IAC	UC	SI	DC	RDF	TRE	RA
650	MUY ALTA	MUY ALTA	MUY ALTA	4	4	4	4	4	4	4
640	MUY ALTA	MUY ALTA	ALTA	4	4	4	3	4	4	4
630	MUY ALTA	MUY ALTA	MEDIA	4	4	4	2	4	3	4
620	MUY ALTA	MUY ALTA	BAJA	4	4	4	1	2	2	4
610	MUY ALTA	ALTA	MUY ALTA	4	4	4	4	4	4	3
600	MUY ALTA	ALTA	ALTA	4	4	4	3	4	4	3
590	MUY ALTA	ALTA	MEDIA	4	4	4	2	3	3	3
580	MUY ALTA	ALTA	BAJA	4	4	4	1	3	3	3
570	MUY ALTA	MEDIA	MUY ALTA	4	4	4	4	3	3	2
560	MUY ALTA	MEDIA	ALTA	4	4	4	3	3	3	2
550	MUY ALTA	MEDIA	MEDIA	4	4	4	2	3	3	2
540	MUY ALTA	MEDIA	BAJA	4	4	4	1	3	3	2
530	MUY ALTA	BAJA	MUY ALTA	4	4	4	4	3	3	1
520	MUY ALTA	BAJA	ALTA	4	4	4	3	3	3	1
510	MUY ALTA	BAJA	MEDIA	4	4	4	2	3	3	1
500	MUY ALTA	BAJA	BAJA	4	4	4	1	3	3	1
490	ALTA	MUY ALTA	MUY ALTA	3	3	3	4	4	4	4
480	ALTA	MUY ALTA	ALTA	3	3	3	3	3	3	4
470	ALTA	MUY ALTA	MEDIA	3	3	3	2	3	3	4
460	ALTA	MUY ALTA	BAJA	3	3	3	1	3	3	4
450	ALTA	ALTA	MUY ALTA	3	3	3	4	3	3	3
440	ALTA	ALTA	ALTA	3	3	3	3	3	3	3
430	ALTA	ALTA	MEDIA	3	3	3	2	3	3	3
420	ALTA	ALTA	BAJA	3	3	3	1	2	2	3
410	ALTA	MEDIA	MUY ALTA	3	3	3	4	2	2	2
400	ALTA	MEDIA	ALTA	3	3	3	3	2	2	2
390	ALTA	MEDIA	MEDIA	3	3	3	2	2	2	2
380	ALTA	MEDIA	BAJA	3	3	3	1	2	2	2
370	ALTA	BAJA	MUY ALTA	3	3	3	4	2	2	1
360	ALTA	BAJA	ALTA	3	3	3	3	2	2	1
350	ALTA	BAJA	MEDIA	3	3	3	2	2	2	1
340	ALTA	BAJA	BAJA	3	3	3	1	2	2	1
330	MEDIA	MUY ALTA	MUY ALTA	2	2	2	4	3	3	4
320	MEDIA	MUY ALTA	ALTA	2	2	2	3	3	3	4
310	MEDIA	MUY ALTA	MEDIA	2	2	2	2	3	3	4
300	MEDIA	MUY ALTA	BAJA	2	2	2	1	3	3	4
290	MEDIA	ALTA	MUY ALTA	2	2	2	4	2	2	3
280	MEDIA	ALTA	ALTA	2	2	2	3	2	2	3
270	MEDIA	ALTA	MEDIA	2	2	2	2	2	2	3
260	MEDIA	ALTA	BAJA	2	2	2	1	2	2	3
250	MEDIA	MEDIA	MUY ALTA	2	2	2	4	2	2	2
240	MEDIA	MEDIA	ALTA	2	2	2	3	2	2	2
230	MEDIA	MEDIA	MEDIA	2	2	2	2	2	2	2
220	MEDIA	MEDIA	BAJA	2	2	2	1	1	2	2
210	MEDIA	BAJA	MUY ALTA	2	2	2	4	2	2	1
200	MEDIA	BAJA	ALTA	2	2	2	3	2	2	1
190	MEDIA	BAJA	MEDIA	2	2	2	2	2	2	1
180	MEDIA	BAJA	BAJA	2	2	2	1	1	1	1
170	BAJA	MUY ALTA	MUY ALTA	1	1	1	4	3	3	4
160	BAJA	MUY ALTA	ALTA	1	1	1	3	3	3	4
150	BAJA	MUY ALTA	MEDIA	1	1	1	2	3	3	4
140	BAJA	MUY ALTA	BAJA	1	1	1	1	3	3	4
130	BAJA	ALTA	MUY ALTA	1	1	1	4	2	2	3
120	BAJA	ALTA	ALTA	1	1	1	3	2	2	3
110	BAJA	ALTA	MEDIA	1	1	1	2	2	2	3
100	BAJA	ALTA	BAJA	1	1	1	1	2	2	3
90	BAJA	MEDIA	MUY ALTA	1	1	1	4	2	2	2
80	BAJA	MEDIA	ALTA	1	1	1	3	2	2	2
70	BAJA	MEDIA	MEDIA	1	1	1	2	2	2	2
60	BAJA	MEDIA	BAJA	1	1	1	1	2	2	2
50	BAJA	BAJA	MUY ALTA	1	1	1	4	1	1	1
40	BAJA	BAJA	ALTA	1	1	1	3	1	1	1
30	BAJA	BAJA	MEDIA	1	1	1	2	1	1	1
20	BAJA	BAJA	BAJA	1	1	1	1	1	1	1

IAC Control de identificación y autenticación	**UC** Control de Uso
SI Integridad de Sistemas	**DC** Confidencialidad de DATOS
RDF Flujo de Datos Restringido	**TRE** Tiempo de Respuesta a Eventos
RA Disponibilidad de Recursos	

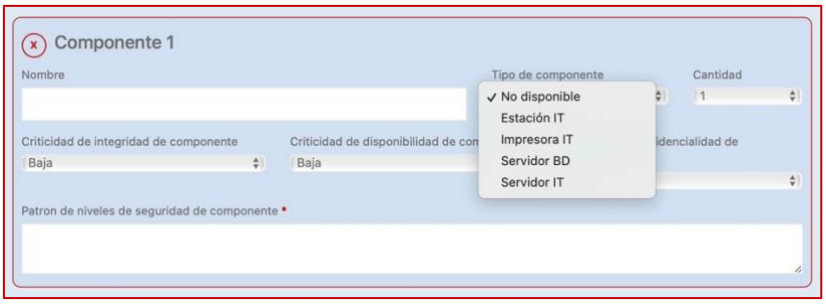
Los números del 1 al 4 se corresponden con los niveles de seguridad de IEC-62443.

A continuación, encontrará una tabla con el significado de cada nivel de seguridad (SL):

Niveles de seguridad (SL)	Significado
0	No tiene requisitos o no precisa protecciones de seguridad
1	Requiere protecciones contra violaciones casuales (errores de la tecnología o fallos humanos)
2	Requiere protecciones contra violaciones intencionadas con pocos recursos, conocimientos generales y baja motivación
3	Requiere protección contra violaciones intencionadas con recursos sofisticados, conocimientos específicos de los Sistemas de Automatización y Control y una moderada motivación.
4	Requiere protección contra violaciones intencionales con recursos sofisticados, conocimientos avanzados de los Sistemas de Automatización y Control y una elevada motivación.

Una vez creada la zona podremos empezar a incorporar componentes de la zona mediante el siguiente botón:

Al igual que al dar de alta una zona, deberemos indicar el nombre del componente, su tipo y la cantidad seleccionando un rango.



El tipo de componente que podremos seleccionar dependerá del tipo de zona, y la cantidad de componentes se seleccionará de un rango.

A continuación, deberá revisar la criticidad del componente, que coincidirá con la criticidad establecida en la zona. Podremos cambiar la criticidad en cualquiera de las dimensiones, para elevarla o reducirla.

Alta de conductos y sus componentes

Dentro del proyecto dará de alta conductos y sus componentes según la arquitectura definida, para ello deberá indicar un nombre de conducto y una descripción. Al igual que en las zonas deberá establecer la criticidad del conducto en cada una de las tres dimensiones.

Una vez establecida la criticidad deberá indicarse la zona origen y la zona destino del conducto y podremos empezar a incorporar componentes del conducto mediante el siguiente botón:

Al igual que al dar de alta un conducto, deberemos indicar el nombre del componente, su tipo y la cantidad seleccionando un rango.

Además del tipo de componente, podrá establecer la cantidad del mismo.

A continuación, deberá revisar la criticidad del componente, que coincidirá con la criticidad establecida en el conducto. Podremos cambiar la criticidad en cualquiera de las dimensiones, para elevarla o reducirla.

Una vez has dado de alta todas las zonas y sus componentes, así como los conductos y sus componentes podrá guardar el proyecto pulsando 

El proceso de envío seguro de la información del proyecto a una base de datos puede tardar unos segundos, dependiendo del tamaño.