

CENTRO DE CIBERSEGURIDAD INDUSTRIAL

EDICIÓN 2022

# ESCIM

## MANUAL DE USO

Caracterización de Incidentes de Alto Impacto en Sistemas Industriales



# 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](mailto:info@cci-es.org)

[www.cci-es.org](http://www.cci-es.org)

Blog: [blog.cci-es.org](http://blog.cci-es.org)

Twitter: [@info\\_cci](https://twitter.com/info_cci)

LinkedIn:

[www.linkedin.com/in/centrociberseguridadindustrial](http://www.linkedin.com/in/centrociberseguridadindustrial)

## **Índice**

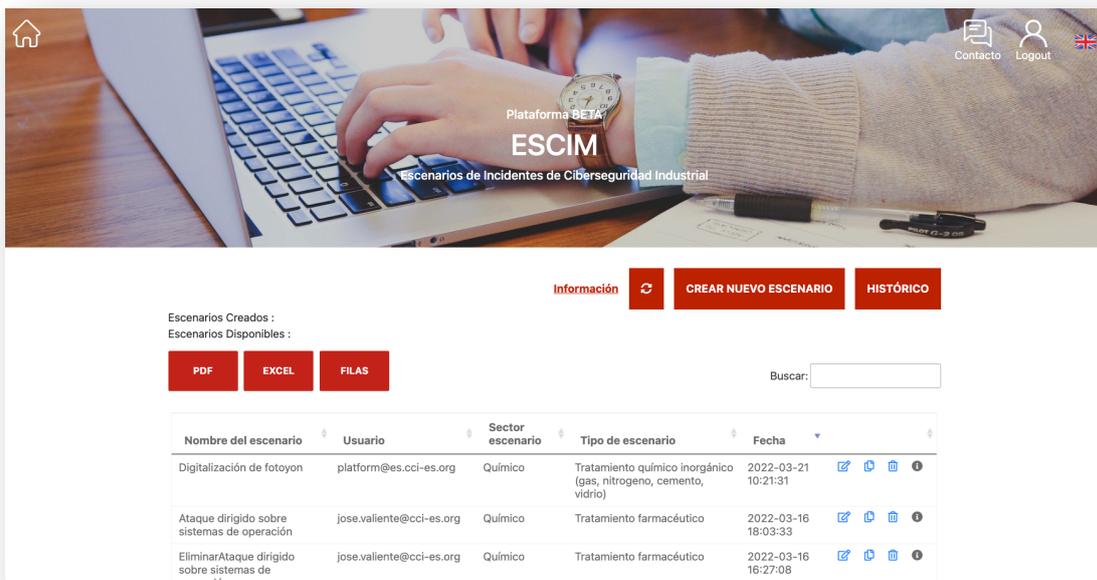
|                                 |          |
|---------------------------------|----------|
| <b>INTRODUCCIÓN</b>             | <b>1</b> |
| <b>CREACIÓN DE UN ESCENARIO</b> | <b>2</b> |
| ALTA DE UNA CARACTERIZACIÓN     | 6        |

## Introducción

ESCIM es una plataforma ágil para facilitar la comprensión y el estudio de incidente de seguridad de alto impacto de Ciberseguridad Industrial a partir de la caracterización de este, bajo el concepto de análisis y comprensión conocido como Tablet Top. A partir de ESCIM, un profesional puede cargar su infraestructura industrial con sus correspondientes zonas y conductos, y añadir una o más caracterizaciones de incidentes tanto internos como externos, para poder avanzar en el análisis y estudio, a partir de los impactos definidos y las necesidades puntuales para cada situación en proyectos de automatización como de digitalización industrial.

ESCIM esta basado en el estándar IEC-62443 como también por la Directiva de Protección de las Redes y Sistemas de Información conocido como en el Reglamento NIS, permitiendo caracterizar el incidente tanto en los aspectos técnicos como también en los niveles de impacto generado. Permite también aprender de las fases de un incidente y conocer para cada caso cuales son los requisitos recomendados para evitarlo o para poder analizarlo mejor.

Para acceder a la plataforma ESCIM 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 ESCIM mediante enlace: <https://escim.cci-es.org/>



The screenshot shows the ESCIM platform interface. At the top, there is a navigation bar with a home icon, a 'Contacto' button, a 'Logout' button, and a language selector (UK flag). The main header area features the text 'Plataforma BETA ESCIM' and 'Escenarios de Incidentes de Ciberseguridad Industrial'. Below this, there are three main navigation buttons: 'Información', 'CREAR NUEVO ESCENARIO', and 'HISTÓRICO'. The 'Escenarios Creados' section shows 'Escenarios Disponibles' with buttons for 'PDF', 'EXCEL', and 'FILAS'. A search bar labeled 'Buscar:' is present. The main content area displays a table of scenarios with the following data:

| Nombre del escenario                                | Usuario                  | Sector escenario | Tipo de escenario  | Fecha               |                              |
|---|--------------------------|------------------|--|---------------------|------------------------------|
| Digitalización de fotoyon                           | platform@es.cci-es.org   | Químico          | Tratamiento químico inorgánico (gas, nitrógeno, cemento, vidrio) | 2022-03-21 10:21:31 | [Edit] [Copy] [Trash] [Info] |
| Ataque dirigido sobre sistemas de operación         | jose.valiente@cci-es.org | Químico          | Tratamiento farmacéutico   | 2022-03-16 18:03:33 | [Edit] [Copy] [Trash] [Info] |
| EliminarAtaque dirigido sobre sistemas de operación | jose.valiente@cci-es.org | Químico          | Tratamiento farmacéutico   | 2022-03-16 16:27:08 | [Edit] [Copy] [Trash] [Info] |

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

La plataforma incorpora un buscador  que te facilitará la localización de los escenarios para poder editarlos mediante , también podrá generar un informe o sumario del escenario con las acciones de prevención y las del Ciclo de Vida de la Gestión de la Respuesta al Incidente 

Desde la pantalla principal podrá borrar escenarios en cualquier momento mediante 

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

| <b>PDF</b> <b>EXCEL</b> <b>FILAS</b>   |             |        |                          |                     | Buscar: <input type="text"/> |
|--|-------------|--------|--------------------------|---------------------|------------------------------|
|  <b>&lt; VOLVER</b> |             |        |                          |                     |                              |
| Nombre del proyecto  | ID Proyecto | Acción | Usuario                  | Fecha               |                              |
| Ataque dirigido sobre sistemas de operación  | 658         | Crear  | jose.valiente@cci-es.org | 2022-03-16 17:03:36 |                              |
| Digitalización de fotoyon  | 661         | Editar | platform@es.cci-es.org   | 2022-03-21 10:21:32 |                              |

## Creación de un Escenario

Para crear un escenario deberá usar **CREAR NUEVO ESCENARIO** y accederá al siguiente formulario:



### Datos del Escenario

Introduzca el nombre del Escenario  
Nombre de escenario de incidente de alto impacto: \*

Seleccione el sector al que pertenece el Escenario  
Seleccione sectores donde aplica el escenario: \*

Selecciona un Sector del Escenario

Seleccione Tipo de Instalación para el Escenario : \*

Otro tipo de instalación industrial

Porcentaje de producción respecto de su sector

Descripción del escenario:  
Descripción general del escenario del incidente (entorno donde se han producido los daños, las consecuencias principales, los canales de acceso, los sistemas comprometidos y los afectados).

Subir arquitectura de zonas y conductos del Escenario: [Plantilla para crear arquitectura](#)

No file chosen

### Caracterizaciones del Incidente

Crea las Caracterizaciones del Escenario

Donde deberá indicar el nombre al Escenario. Si quieres crear una plantilla, le recomendamos que el nombre del escenario 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 escenario. Si no apareciese el sector de su escenario, deberá enviar un email a [escim@cci-es.org](mailto:escim@cci-es.org) para indicar su sector y los tipos de instalaciones que necesita. En menos de 24 horas daremos de alta tu sector y los tipos de instalaciones, avisándote por email de su incorporación.

### Datos del Escenario

**Introduzca el nombre del Escenario**

Nombre de escenario de incidente de alto impacto: \*

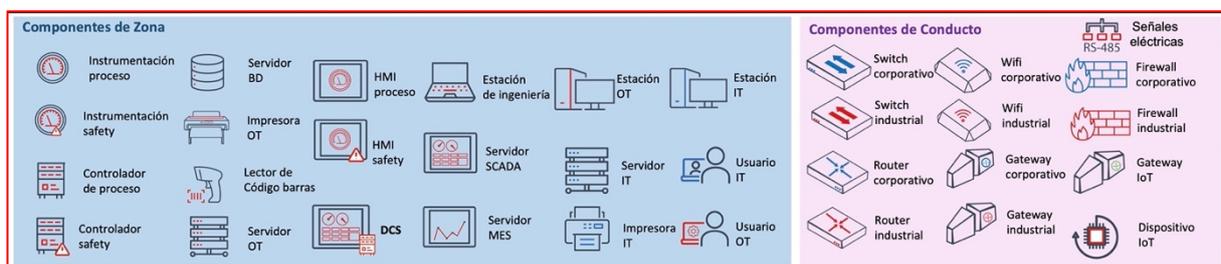
**Seleccione el sector al que pertenece el Escenario**

Seleccione sectores donde aplica el escenario: \*

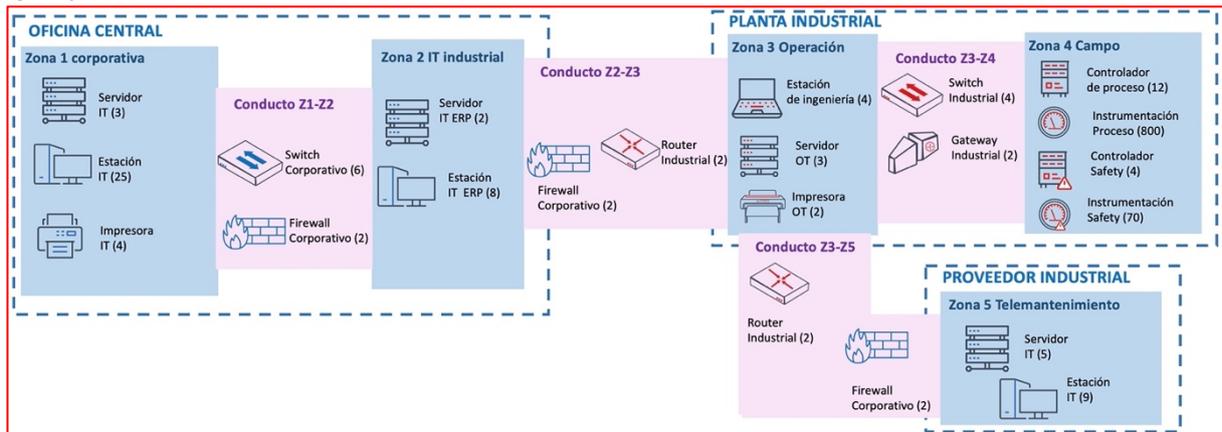
**Seleccione Tipo de Instalación para el Escenario Eléctrico: \***

- Subestación eléctrica
- Ciclo combinado
- Supervisión de generación térmica
- Gestión de Parques
- Automatización de sistemas (PMS, EMS, PCS)
- DIGITALIZADA N(MES, Mant predictivo... )
- Termosolar
- Tratamiento de carbón
- Generador eólico
- EDAR
- Automatización de sistema de alarmas

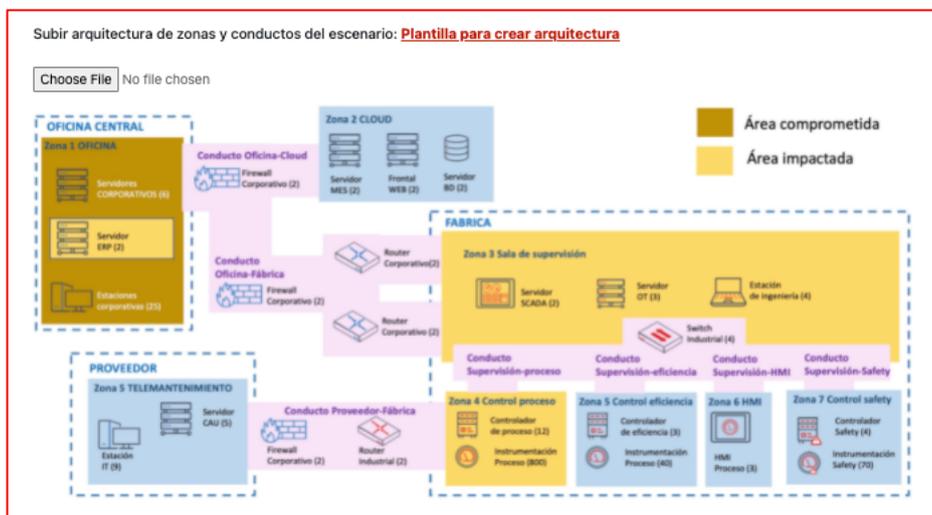
Una vez haya introducido el nombre del Escenario, su sector y el tipo deberá indicar la descripción del Escenario (por ejemplo: Estudiaremos el caso de un Ransomware que ingresa por medio de **XX** y logra afectar a los servidores **ZZ** y las estaciones de ingeniería **YY**...), luego deberá cargar una arquitectura básica que incluya zonas y conductos de su escenario y todos los tipos de componentes para ello dispones de una plantilla en ppt que podrá descargar desde: [Plantilla para crear arquitectura](#) donde encontrará todos los componentes y ejemplo para preparar la arquitectura de su proyecto:



Ejemplo:



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 tráfico 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 una Caracterización

Dentro del Escenario, el primer paso es crear una caracterización y para ello deberá utilizar el botón + Añadir Caracterización y podrá así ver el formulario que le permite cargar la información relativa al tipo de Incidente que se desea caracterizar (su origen, si fue intencional o no, los niveles de peligrosidad...):

x **Caracterización 1**

|  |  |
|--|--|
| <b>Origen</b>  | <b>Tipo</b>  |
| <input type="radio"/> Interno <input checked="" type="radio"/> Externo <input type="radio"/> Interno+Externo | <input checked="" type="radio"/> Intencionado <input type="radio"/> Accidental <input type="radio"/> Desconocido |

**Amenazas Externo**

- Robo de medios físicos o lógicos
- Alteración de información en soporte o tránsito
- No disponibilidad de personal externo
- Fallo de servicio de soporte (comunicaciones, electricidad, mantenimiento)
- Estado
- Hacking
- Ransomware
- Malware
- Ingeniería social
- Competencia
- Proveedor comprometido
- Proveedor comprometido

**NIVELES DE PELIGROSIDAD DEL INCIDENTE (REGLAMENTO NIS)**

**Nivel Crítico**

APT

**Nivel Muy Alto**

|   |  |   |
|---|--|---|
| <input type="radio"/> Distribución de malware | <input type="radio"/> Configuración de malware | <input type="radio"/> Robo (intrusión física) |
| <input type="radio"/> Sabotaje                | <input type="radio"/> Interrupciones           |   |

**Nivel Alto**

|   |  |
|---|--|
| <input checked="" type="radio"/> Acceso no autorizado a información | <input type="radio"/> Ataque desconocido   |
| <input type="radio"/> Compromiso de aplicaciones                    | <input type="radio"/> Compromiso de cuentas con privilegios                        |
| <input type="radio"/> DDoS (Denegación distribuida de servicio)     | <input type="radio"/> DoS (Denegación de servicio)                                 |
| <input type="radio"/> Modificación no autorizada de información     | <input type="radio"/> Pérdida de datos   |
| <input type="radio"/> Phishing                                      | <input type="radio"/> Pornografía infantil, contenido sexual o violento inadecuado |
| <input type="radio"/> Servidor C&C (Command & Control)              | <input type="radio"/> Sistema infectado  |

Pero también podrá cargar en el mismo formulario información relacionada con los niveles de impacto al negocio, impacto técnico y el impacto según las definiciones del Reglamento NIS:

**IMPACTO PARA EL NEGOCIO**

Descripción de impacto para el negocio:

Identificar las pérdidas para el negocio, económicas, reputacional, calidad, vidas

Impacto Operativo: Muy Alto (v)

Impacto Patrimonial: Medio (v)

Impacto Reputacional: Bajo (v)

Impacto Legal: Alto (v)

Impacto Financiero: Alto (v)

Impacto Salud y/o medioambiente: Muy Alto (v)

[Consultar tabla de valoración de impactos \(por sectores\)](#)

**IMPACTO TÉCNICO**

Descripción de impacto técnico:

Identificar las pérdidas de servicio y el tiempo que se requiere para su recuperación

Perdida de disponibilidad sufrida: Alto (v)

Perdida de integridad sufrida: Alto (v)

Perdida de confidencialidad sufrida: Muy Alto (v)

[Consultar tabla de valoración de pérdidas \(por sectores\)](#)

**IMPACTO (REGLAMENTO NIS)**

**Impacto Crítico**

Daños reputacionales muy elevados ●

Interrupción en prestación del servicio >24 h ●

Afecta con peligro a la vida de las personas ○

Resolución de incidente > 100 J-persona ○

Afecta a una infraestructura crítica ○

Afecta apreciablemente a seguridad nacional ○

**Impacto Muy Alto**

Daños reputacionales elevados ○

Interrupción en prestación del servicio >8 h ●

Afecta apreciablemente a actividades oficiales ○

Resolución de incidente > 30 J-persona ○

Afecta a un servicio esencial ○

Afecta a seguridad ciudadana bienes materiales ●

**Impacto Alto**

Daños reputacionales de difícil reparación ○

Interrupción en prestación del servicio >1 h ○

Resolución de incidente > 5 J-persona ○

Afecta a un operador ○

También puede incluir una descripción de lo sucedido en cada una de las fases como los tiempos de cada una de ella, incluso identificar las fuentes de registro del incidente con las que se cuenta:

**FASES DEL INCIDENTE (INCORPORAR TIEMPOS DE CADA FASE)**

|  |   |
|--|---|
| <p><b>Fase 1. Paciente cero</b></p> <p>Han entrado</p> <p>entre 24 y 72 Hs</p>                             | <p><b>Fase 2. Acceso inicial</b></p> <p>A través del proveedor del servicio de soporte.</p> <p>entre 2 y 8 Hs</p> |
| <p><b>Fase 3. Persistencia</b></p> <p>Esperando oportunidad</p> <p>más de 72 Hs</p>                        | <p><b>Fase 4. Efectos</b></p> <p>Alterando los niveles del flujo del control operativo</p> <p>entre 2 y 8 Hs</p>  |
| <p><b>Fase 5. Actuaciones post-incidente</b></p> <p>Desconexión de acceso remoto</p> <p>entre 2 y 8 Hs</p> |   |

**Fuentes de registro del incidente recomendadas:**

Logs de firewalls     
 Grabaciones de las cámaras de vigilancia     
 Log de sistemas ICS  
 Logs de antimalware     
 Logs de sistema de correo     
 Registro de personal de seguridad  
 Logs de equipos de comunicaciones

Una vez definidas las bases del incidente, queda determinar cuales serán las zonas comprometidas y cuáles las zonas impactadas, con sus componentes, niveles de criticidades, patrones de niveles de seguridad implementados y los deseados (según IEC-62443)

Para comenzar a añadir la información de las zonas comprometidas e impactadas, dispone del

botón + Añadir zona comprometidas o del botón + Añadir zona impactada que desplegará el correspondiente formulario:

**Zonas comprometidas**

**Zona Comprometida 1**

Nombre de zona: Mantenimiento remoto      Tipo de zona: Zona corporativa con componentes de nivel 4

Descripción de zona: Sistemas

Patrón de niveles de seguridad existente para la zona comprometida: Patrón 200 - Disponibilidad (Baja) Integridad (Alta) Confidencialidad (Alta) - IAC[3] UC[3] SI[3] DC[3] RDF[2] TRE[2] RA[1]

Criticidad de integridad de zona: Muy Alta      Criticidad de disponibilidad de zona: Media      Criticidad de confidencialidad de zona: Baja

Patrón de niveles de seguridad recomendado para la zona comprometida: Patrón:540 - Integridad (Muy Alta) Disponibilidad (Media) Confidencialidad (Baja) IAC[ 4 ] UC[ 4 ] SI[ 4 ] DC[ 1 ] RDF[ 3 ] TRE[ 3 ] RA[ 2 ]

**Zonas impactadas**

**Zona Impactada 1**

Nombre de zona: Campo      Tipo de zona: Zona corporativa con componentes de nivel 4

Descripción de zona: Control de turbina

Patrón de niveles de seguridad existente para la zona comprometida: Patrón 250 - Disponibilidad (Alta) Integridad (Alta) Confidencialidad (Baja) - IAC[3] UC[3] SI[3] DC[2] RDF[2] TRE[2] RA[3]

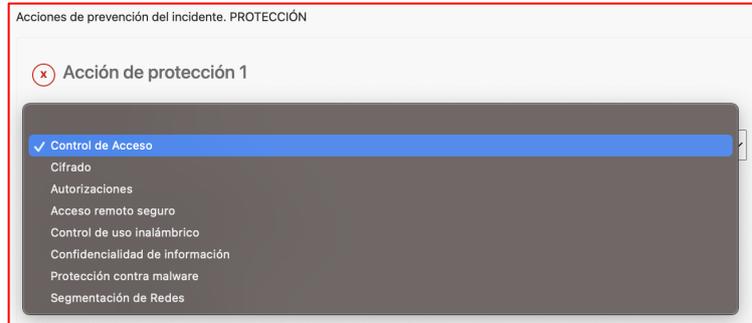
Criticidad de integridad de zona: Alta      Criticidad de disponibilidad de zona: Alta      Criticidad de confidencialidad de zona: Alta

Patrón de niveles de seguridad recomendado para la zona impactada: Patrón:440 - Integridad (Alta) Disponibilidad (Alta) Confidencialidad (Alta) IAC[ 3 ] UC[ 3 ] SI[ 3 ] DC[ 3 ] RDF[ 3 ] TRE[ 3 ] RA[ 3 ]

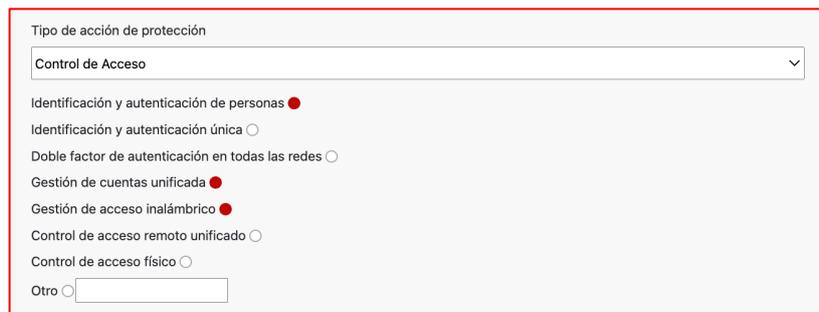
A partir de este momento, podrá cargar la información relativa a las acciones de PREVENCIÓN de un incidente de seguridad, las cuales se dividen en:

+ Añadir acción de identificación     
+ Añadir acción de protection

Y en cada acción que decida añadir podrá identificar además de la acción en sí, una o más tareas (dependiendo el caso) relacionadas con el tipo de acción definida. Por ejemplo, si selecciona “+Añadir acción de Protección” tendrá que seleccionar de un menú desplegable cuál tipo de acción desea añadir:



Y al seleccionar el “Tipo de acción” se mostrarán las tareas para esa acción específica, como puede verse en el siguiente ejemplo:



Una vez completada las acciones de PREVENCIÓN, deberá ingresar la información correspondiente a las acciones del CICLO DE VIDA de la Gestión de Respuesta al Incidente, y para ello deberá seguir la misma metodología anteriormente mencionada, pero utilizando los botones correspondientes:



Al igual que en las acciones de PREVENCIÓN, para los tipos de acciones definidos en el Ciclo de Vida de la Gestión de Respuesta al Incidente, tendrá la opción de seleccionar cuales tareas específicas deberían llevarse a cabo ante este tipo de situaciones:



Una vez has dada de alta toda la información relativa al incidente (datos del sector, zonas comprometidas y zonas impactadas), a la caracterización y a los tipos de acciones podrá guardar el Escenario pulsando



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