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

www.cci-es.org

Blog: blog.cci-es.org

Twitter: @info_cci

LinkedIn: www.linkedin.com/in/centrociberseguridadindustrial

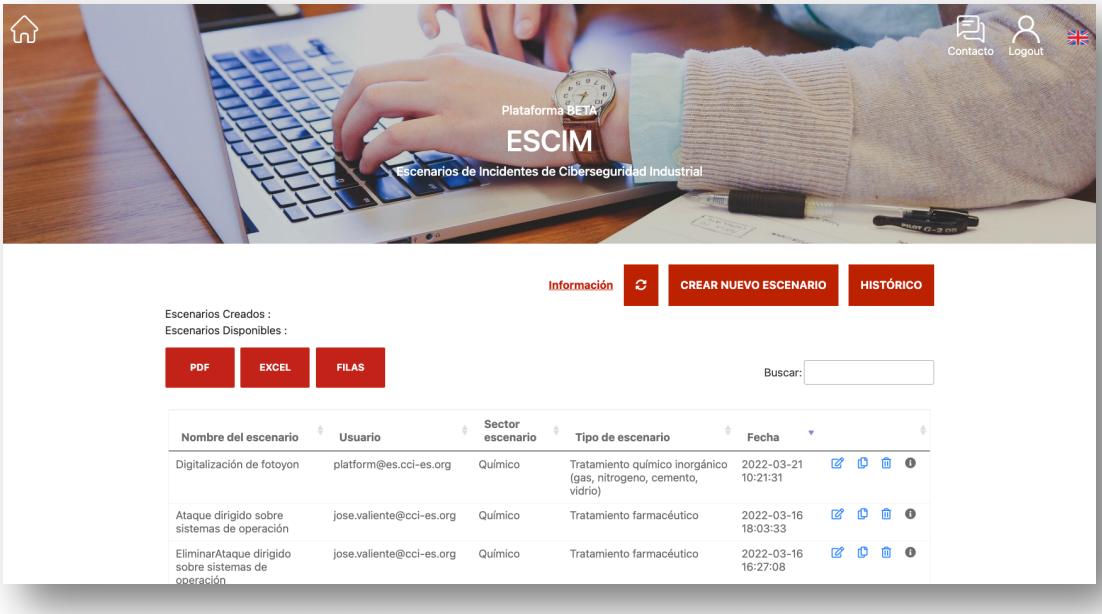
Índice

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/

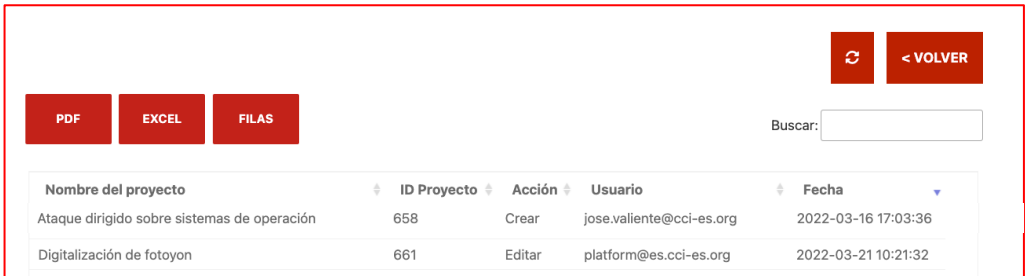


Con esta plataforma podrá crear escenarios o caracterizaciones desde cero o crear plantillas que podrán utilizarse como base para tus nuevos escenarios, para ello simplemente debes crear un proyecto y copiarlo tantas veces como lo necesites usando 

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 

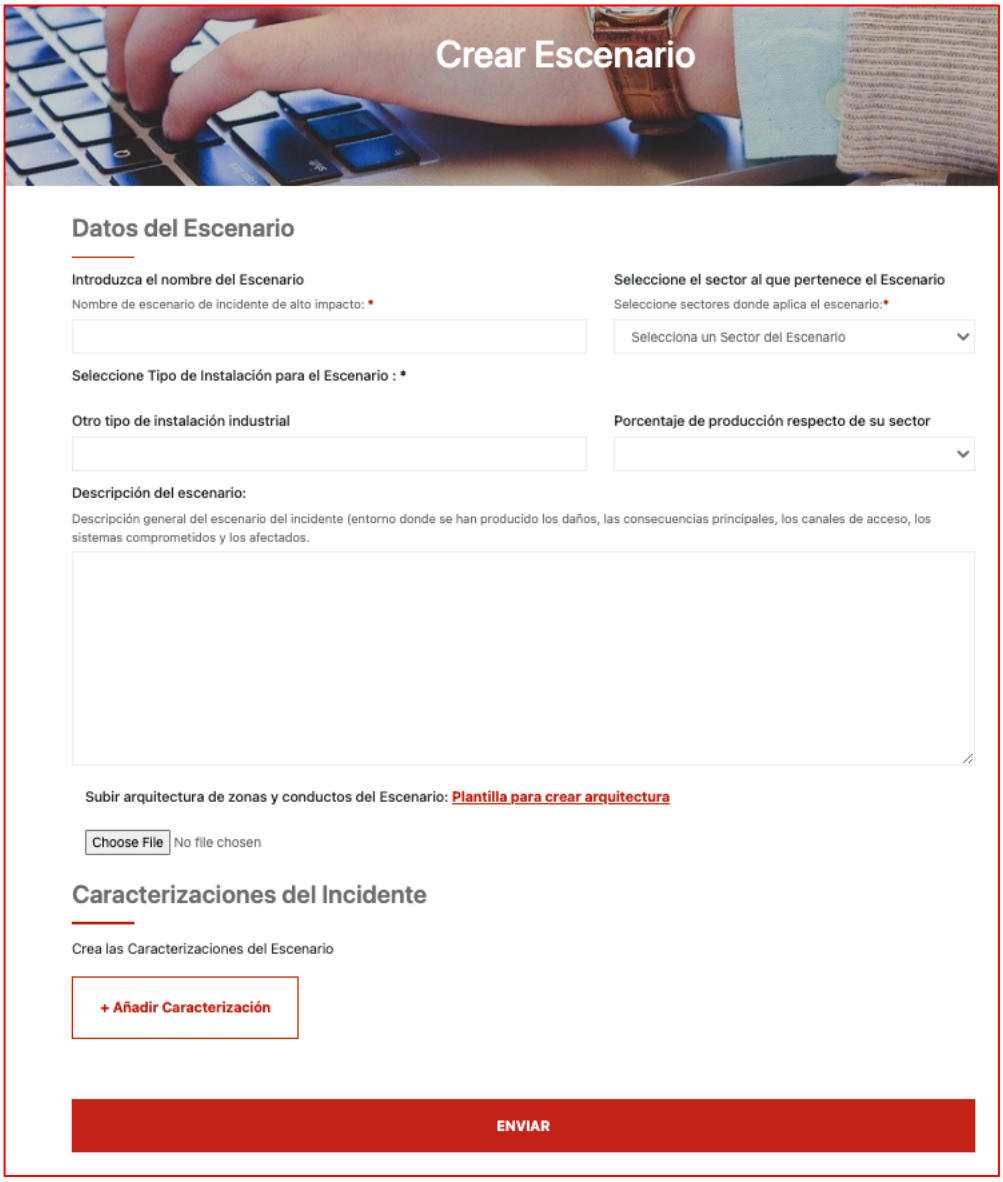
Desde la pantalla principal podrá borrar escenarios en cualquier momento mediante  .

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



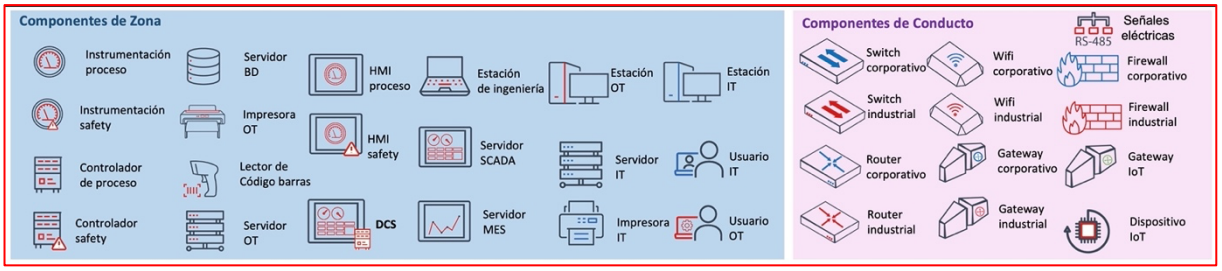
Creación de un Escenario

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

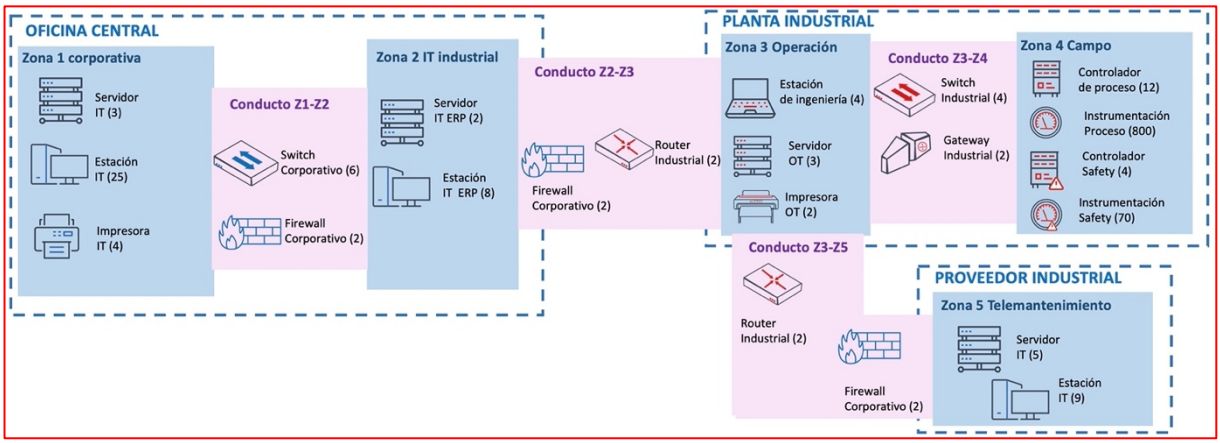


Donde deberá indicar el nombre al Escenario. Si quieres crear una plantilla, le recomendamos que el nombre del escenario empiece por “Plantilla – XXX” lo cual te facilitará la búsqueda de plantillas. Una vez indicado el nombre, deberá seleccionar el sector al que pertenece su escenario. Si no apareciese el sector de su escenario, deberá enviar un email a escim@cci-es.org 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.

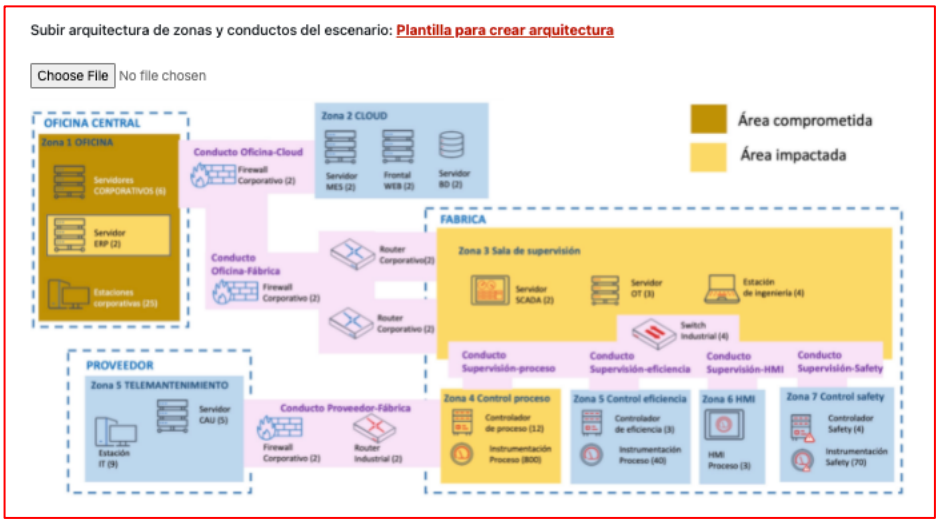
Una vez haya introducido el nombre del Escenario, su sector y el tipo deberá indicar la descripción del Escenario (por ejemplo: Estudiaremos el caso de un Ransomware que ingresa por medio de XX y logra afectar a los servidores ZZ y las estaciones de ingeniería YY…), luego deberá cargar una arquitectura 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.

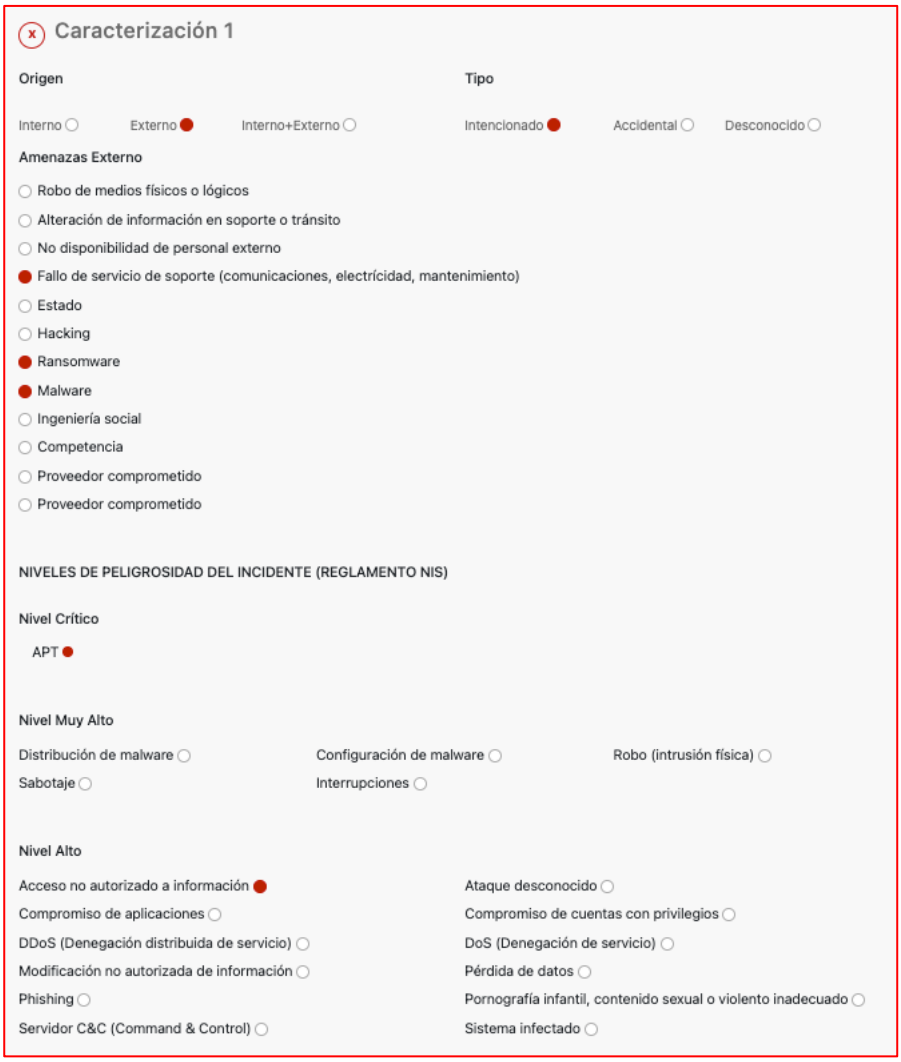
- Los activos identificados como Sistemas Instrumentados de Seguridad (SIS) deben estar en Zonas distintas. Los SIS por su naturaleza poseen requisitos de seguridad diferentes a los demás componentes de un sistema de control industrial.

- 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 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.

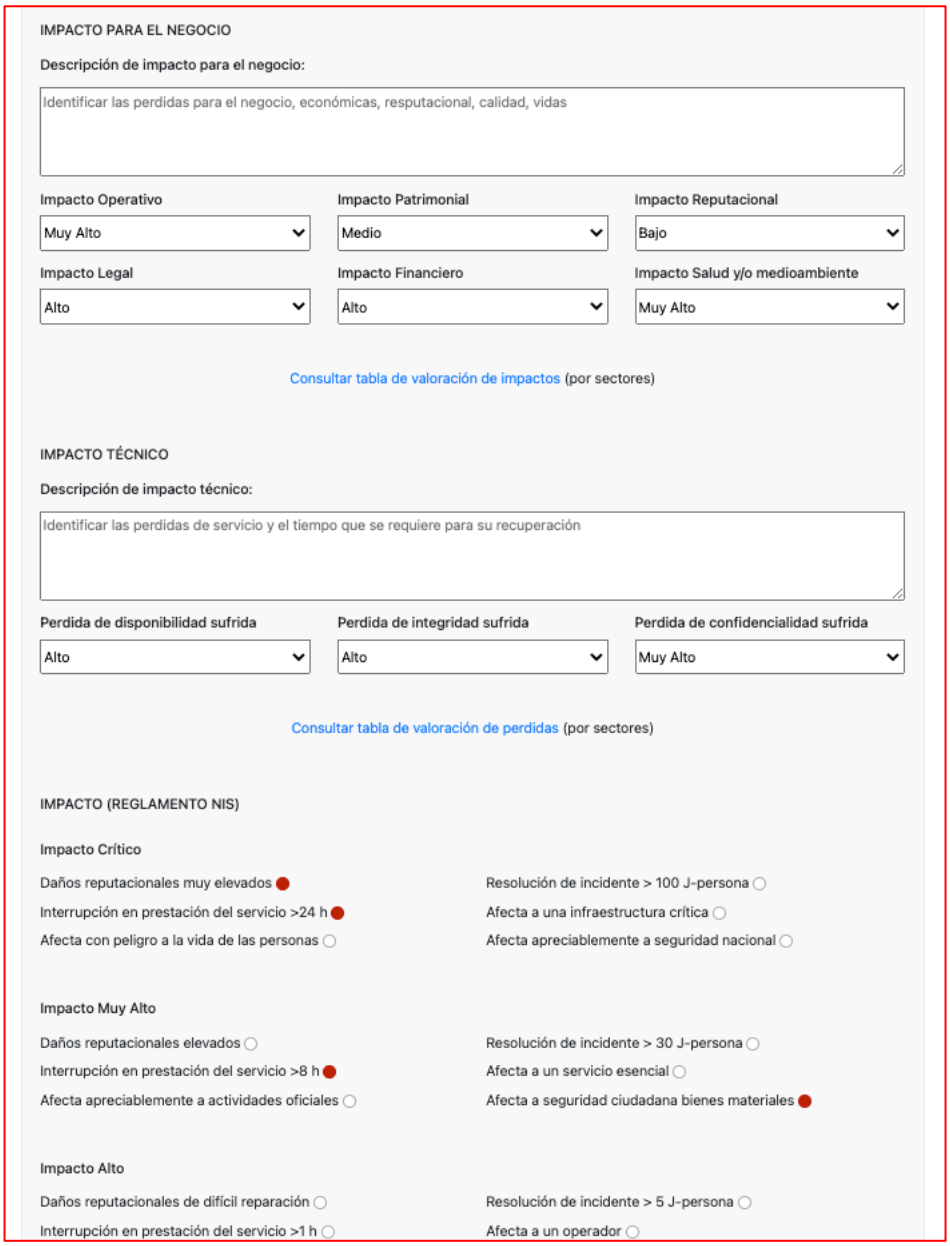
- Las comunicaciones inalámbricas deben ubicarse en una o más zonas separadas de las comunicaciones cableadas. Las comunicaciones inalámbricas no son controladas por muros o gabinetes y por lo tanto poseen un mayor nivel de exposición que las comunicaciones cableadas.

Alta de una Caracterización

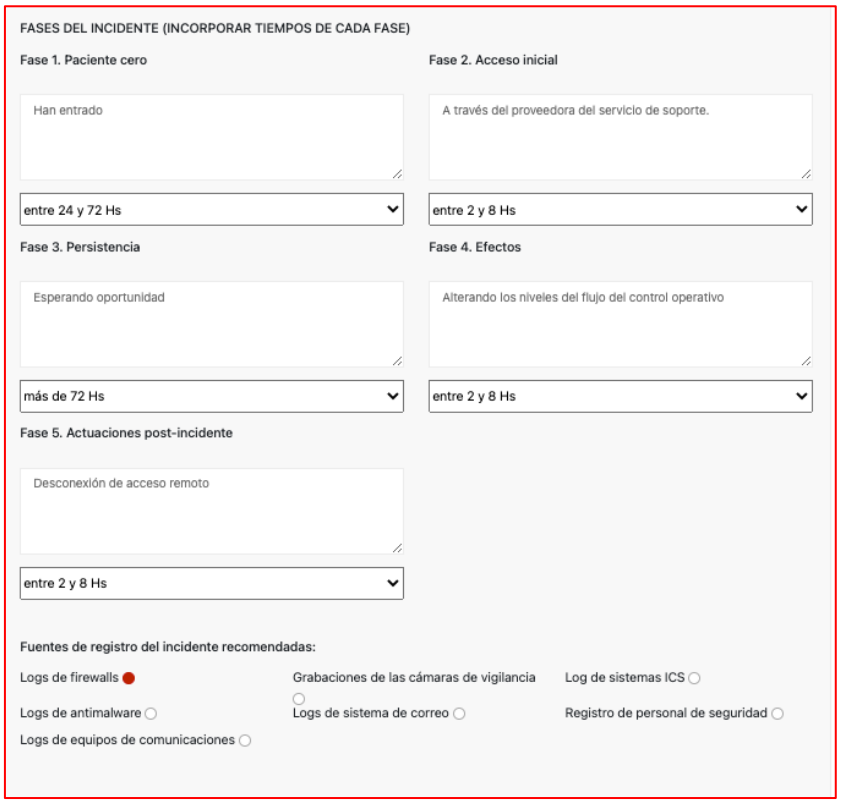
Dentro del Escenario, el primer paso es crear una caracterización y para ello deberá utilizar el botón + Añadir Caracterización y podrá así ver el formulario que le permite cargar la información relativa al tipo de Incidente que se desea caracterizar (su origen, si fue intencional o no, los niveles de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



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:

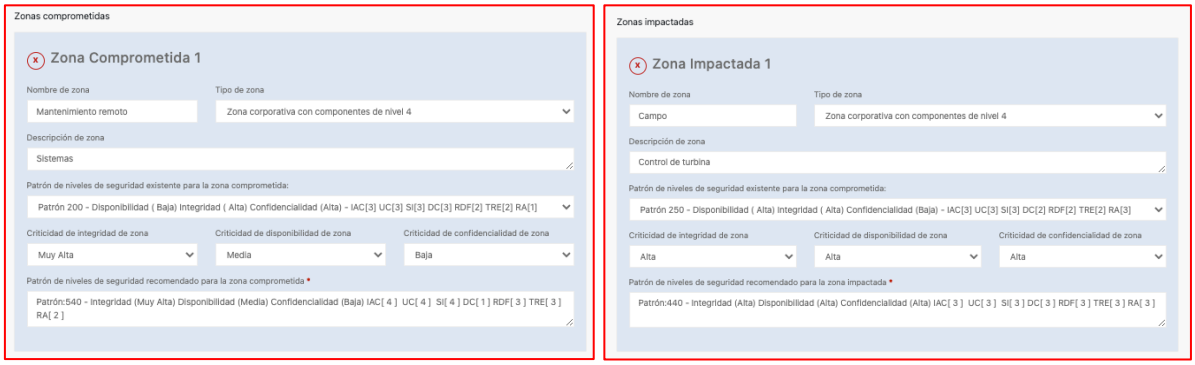


También puede incluir una descripción de lo sucedido en cada una de las fases como los tiempos de cada una de ella, incluso identificar las fuentes de registro del incidente con las que se cuenta:



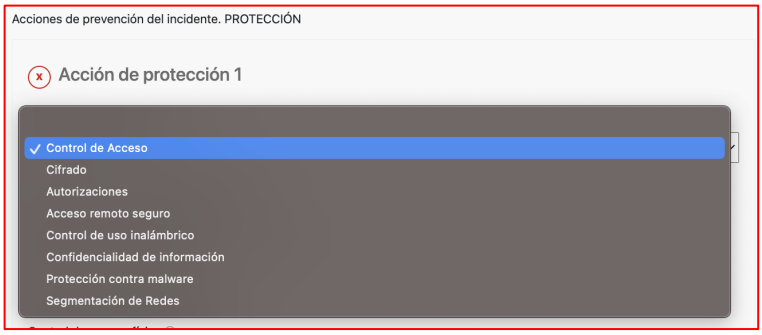
Una vez definidas las bases del incidente, queda determinar cuales serán las zonas comprometidas y cuáles las zonas impactadas, con sus componentes, niveles de criticidades, patrones de niveles de seguridad implementados y los deseados (según IEC-62443)

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:

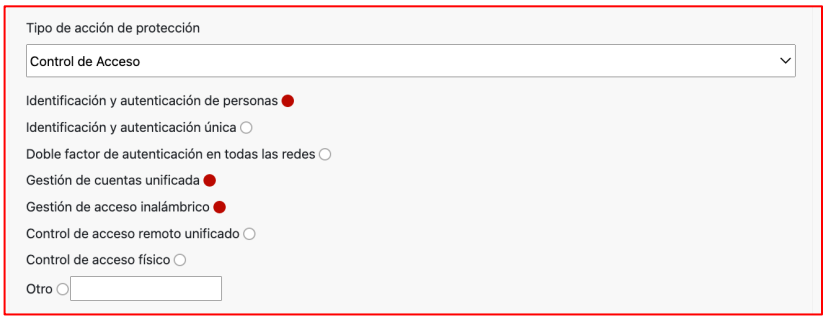


A partir de este momento, podrá cargar la información relativa a las acciones de PREVENCION de un incidente de seguridad, las cuales se dividen en:

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 PREVENCION, 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 PREVENCION, 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.