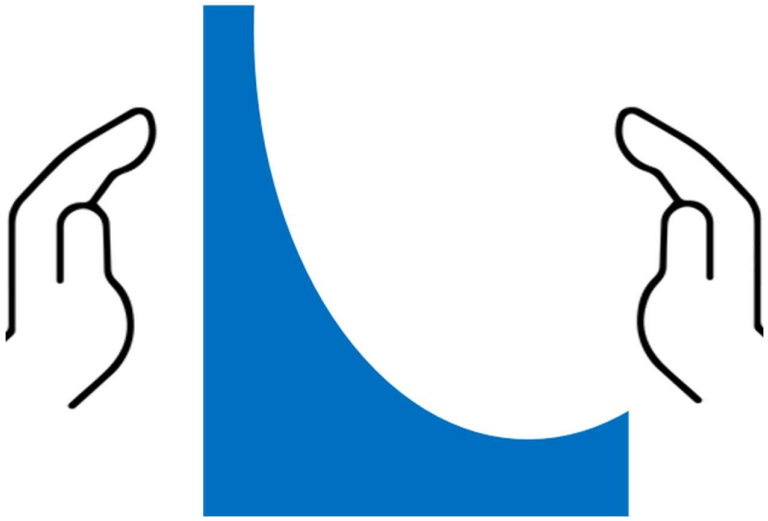

GUÍA TÉCNICA DE PROTECCIÓN DE INFRAESTRUCTURAS HIDRÁULICAS ESTRATÉGICAS

Versión divulgación

Junio 2024.

PROLOGO

La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (IICC), tiene como objeto establecer las estrategias y las estructuras organizativas adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las administraciones públicas en materia de protección de infraestructuras críticas.

Dicha Ley tiene su desarrollo mediante el Real Decreto 704/2011 de 20 de mayo, por el que aprueba el Reglamento de medidas para la protección de las infraestructuras críticas.

Esta normativa estatal define los Operadores Críticos como las entidades u organismos responsables del funcionamiento de las IICC, que en el Sector Estratégico del Agua fueron designados en septiembre de 2015.

Estos Operadores Críticos deben elaborar un Plan de Protección Específico para cada Infraestructura Crítica, para lo cual cuentan con una Guía de buenas prácticas elaborada por la Secretaría de Seguridad del Ministerio de Interior.

Sin embargo, no existe para el mundo de las presas, una guía que afronte este reto desde un punto de vista ingenieril, estableciendo los modos de fallo, no sólo de la seguridad física y cibernética, sino involucrando también la seguridad estructural.

Esta "*Guía técnica de protección de infraestructuras hidráulicas estratégicas*" editada por el Comité Nacional Español de Grandes Presas, pretende servir de soporte a los Operadores en el diseño de las medidas de protección de sus infraestructuras.

De esta guía existen dos versiones, una completa para operadores y otra reducida para divulgación. La versión aquí contenida corresponde a la segunda de ellas y por razones de seguridad su contenido ha sido restringido.

En la elaboración de la presente Guía han participado los siguientes integrantes del Comité Nacional Español de Grandes Presas:

Gómez López de Munain, René. (Director).

Echeverría García, Eduardo. (Secretario Técnico).

Castillo Rodríguez, Jessica Tamara.

De Cea Azañedo, Juan Carlos.

Domínguez Domínguez, María.

Escuder Bueno, Ignacio.

Garcia del Valle, David.

Gómez de Membrillera Ortuño, Manuel.

González Tejada, Ignacio.

Granados García, Alfredo.

Navarro Carrasco, Óscar.

Olalla Marañón, Claudio.

Rojo Martínez, Eduardo.

Aunque todos los miembros han revisado el contenido completo de la guía, cada capítulo ha sido coordinado por uno o varios miembros, según la siguiente relación:

Casos históricos	René Gómez López de Munain.
Fallo de control de accesos	Eduardo Echeverría García.
Corte de acceso físico	Alfredo Granados García y David García del Valle.
Ataque con drones	María Domínguez Domínguez.
Sabotaje por personal propio	Eduardo Rojo Martínez.
Accionamiento malintencionado de compuertas	Jessica Tamara Castillo Rodríguez e Ignacio Escuder Bueno.
Voladura o deterioro grave	Ignacio González Tejada y Claudio Olalla Marañón.
Sabotaje del sistema de drenaje	Manuel Gómez de Membrillera Ortuño.
Ciberseguridad/ riesgos ciberfísicos	Óscar Navarro Carrasco.
Contaminación intencionada del agua	René Gómez López de Munain.

A todos los componentes del Comité de Protección de Infraestructuras Hidráulicas Estratégicas les agradecemos sinceramente su esfuerzo y dedicación para hacer posible la elaboración de esta Guía, que esperamos sea de utilidad.

Carlos Granell Ninot

Presidente del Comité Nacional Español de Grandes Presas (SPANCOLD)

INDICE

INDICE DE ILUSTRACIONES

1 INTRODUCCIÓN

Los servicios esenciales que se prestan a la sociedad descansan sobre una serie de infraestructuras de gestión, tanto pública como privada, cuyo funcionamiento es indispensable. Así las **Infraestructuras Estratégicas** son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

Si además estas infraestructuras estratégicas no permiten soluciones alternativas, se denominan **Infraestructuras Críticas (IICC)**.

Las obras hidráulicas, a efectos de esta clasificación, se engloban en el Sector Estratégico del Agua pudiendo incluir infraestructuras como redes de distribución, canales, potabilizadoras, presas y embalses, etc. Su perturbación o destrucción tendría un grave impacto, por lo que se hace necesario el diseño de una política de seguridad homogénea e integral que las proteja.

Así lo entendieron tras los efectos devastadores de las Segunda Guerra Mundial, cuando en el Protocolo I adicional a los "***Convenios de Ginebra de 1949***" relativo a la "*protección de las víctimas de los conflictos armados internacionales*", de 1977, se hace una mención específica a las presas en su artículo 56 de Protección de las obras e instalaciones que contienen fuerzas peligrosas y que se reproduce a continuación:

"*1. Las obras o instalaciones que contienen fuerzas peligrosas, a saber, las **presas, los diques** y las centrales nucleares de energía eléctrica, **no serán objeto de ataques, aunque sean objetivos militares**, cuando tales ataques puedan producir la liberación de aquellas fuerzas y causar, en consecuencia, pérdidas importantes en la población civil. Los otros objetivos militares ubicados en esas obras o instalaciones, o en sus proximidades, no serán objeto de ataques cuando tales ataques puedan producir la liberación de fuerzas peligrosas y causar, en consecuencia, pérdidas importantes en la población civil.*

Tras los atentados de Madrid del 11 de marzo de 2004, el Consejo Europeo aprobó el Programa europeo de protección de infraestructuras críticas (PEPIC) y puso en marcha una red de información sobre alertas en infraestructuras críticas.

España comenzó su incursión en la protección de las Infraestructuras Críticas con la creación del primer Plan Nacional de Protección de las Infraestructuras Críticas, de 7 de mayo de 2007, y la elaboración del primer Catálogo Nacional de Infraestructuras Estratégicas agrupadas por sectores.

Con posterioridad los estados miembros de la Unión Europea desarrollaron la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección. En dicha Directiva se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los Estados miembros y a los operadores de las mismas, y se determina el desarrollo de una serie de obligaciones y de actuaciones a desarrollar por cada país.

Con la misma finalidad, el gobierno español desarrolló la Ley 8/2011, de 28 de abril por la que se establecen medidas para la protección de las infraestructuras críticas, que

tiene como objeto establecer las estrategias y las estructuras organizativas adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las administraciones públicas en materia de protección de infraestructuras críticas.

Dicha Ley tiene su desarrollo mediante el Real Decreto 704/2011 de 20 de mayo, por el que aprueba el Reglamento de medidas para la protección de las infraestructuras críticas.

Esta normativa estatal define los Operadores Críticos como las entidades u organismos responsables del funcionamiento de la IICC, que en el Sector Estratégico del Agua fueron designados en septiembre de 2015.

Según la normativa vigente el Operador debe elaborar un Plan de Protección Específico (PPE) por cada una de las infraestructuras críticas, en el plazo de cuatro meses desde la aprobación del Plan de Seguridad del Operador (PSO). Es el documento operativo donde se deben definir las medidas concretas ya adoptadas y las que vaya a adoptar el operador para garantizar la seguridad integral (física y lógica) de cada una de sus infraestructuras críticas.

El Secretario de Estado de Seguridad estableció, a través del Centro Nacional para la Protección de las Infraestructuras críticas mediante Resolución de 8 de septiembre de 2015, los "*Contenidos mínimos del Plan de Protección Específico*", con los que debe contar todo PPE, así como el modelo en el que fundamentar su estructura y compleción.

Con posterioridad, la Secretaría de Estado de Seguridad editó la "*Guía de Buenas Prácticas del Plan de Protección Específico*", documento de carácter voluntario que no incluye requisitos adicionales a los establecidos por la legislación vigente, con la intención de facilitar la aplicación de estas buenas prácticas.

La presente Guía tiene por objetivo, cumpliendo con los documentos anteriores, desarrollar dos aspectos esenciales del Plan de Protección Especifico aplicable a las IICC, pero que también tiene cabida en las Infraestructuras hidráulicas Estratégicas:

- El análisis de los riesgos, en especial las amenazas consideradas, relacionándolas con los modos de fallo de la infraestructura.
- Las medidas de protección (organizativas, operacionales o técnicas) a implementar en la infraestructura.

Es innegable admitir que, aunque el enfoque del tratamiento abarca a todas las infraestructuras hidráulicas, el sesgo profesional de los autores hace que las infraestructuras de regulación tengan una consideración principal.

2 DEFINICIONES O GLOSARIO

A continuación, se van a describir algunos términos y acrónimos utilizados en el documento y cuya definición es importante esté aclarada, para tener una correcta comprensión de la Guía.

a) Activo crítico

Aquellos recursos, elementos y sistemas de una infraestructura que son esenciales e imprescindibles para mantener y desarrollar las capacidades y operatividad de la misma, o que están destinados a cumplir dicho fin.

b) Análisis de Riesgos.

Estudio de las hipótesis de amenazas posibles, necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo. (Fuente: artículo 2 de la ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas). En el apartado 5.2 se hace una enumeración de los diferentes activos y amenazas que se incluyen en el análisis de riesgos.

c) Infraestructuras estratégicas

Las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales. (Fuente: artículo 2 de la ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas).

d) Infraestructuras críticas

Las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. (Fuente: artículo 2 de la ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas).

e) Modo de fallo

Secuencia particular de eventos que puede dar lugar a un funcionamiento inadecuado del sistema presa - embalse o una parte del mismo. Esta serie de sucesos se asocia a un determinado escenario de solicitación y tiene una secuencia lógica, la cual consta de un evento inicial desencadenante, una serie de eventos de desarrollo o propagación y culmina con el fallo de la presa.

Dependiendo del alcance y objetivo del análisis, se puede restringir la definición del modo de fallo a aquellos que impliquen potencialmente la pérdida de vidas humanas o incluir cualquier modo de fallo con potencial para producir un vertido incontrolado de caudales y por tanto con potencial para causar daños de cualquier tipo (económicos, sobre la vida humana, medioambiente, etc.) e incluso cualquier mecanismo que provoque algún tipo de daño (incluso sin necesidad de que se produzca un vertido), por ejemplo uno que origine consecuencias económicas por pérdida de misión. Así mismo, el análisis de los modos de fallo no se ciñe exclusivamente a las estructuras de retención de un embalse, sino que tiene en cuenta cualquier elemento incluido en el sistema

presa-embalse. (Fuente: Guía técnica de seguridad de presas Nº 8: Análisis de riesgos aplicado a la gestión de seguridad de presas y embalses).

f) Riesgo

Combinación de la probabilidad de que se produzca un evento y de sus posibles consecuencias negativas para la salud humana, la actividad económica, el medio ambiente, las infraestructuras, el patrimonio cultural, etc.

Riesgo = Peligrosidad x Exposición x Vulnerabilidad= Σ[P(Suceso)*P(Consecuencias) *P(Daños)]

En el mundo de la ingeniería de presas se utiliza con mayor frecuencia la expresión “modo de fallo”, pudiendo una misma amenaza afectar a varios modos de fallo. Por ejemplo, el ataque masivo con explosivos, puede producir dos modos de fallo: afección a compuertas, y daños del cuerpo de presa. En el apartado 5.1 se describe una metodología para su cálculo y clasificación en función de su impacto y probabilidad de ocurrencia

g) Peligrosidad

Peligrosidad, peligro o amenaza: probabilidad de ocurrencia de un evento o secuencia de eventos, natural o antrópico potencialmente perjudicial. Es la inversa del Periodo de Retorno. En el Anexo I aparece un listado de las amenazas más frecuentes.

h) Exposición

Descripción de los daños o consecuencias que una amenaza ocasiona para la población, edificaciones, obras de ingeniería civil, actividades económicas, servicios públicos, elementos medioambientales y otros usos del territorio expuestos.

i) Vulnerabilidad

Probabilidad de ocurrencia de los daños anteriores.

j) Nivel de Riesgo Inherente

Determina el nivel de riesgo que tiene un activo o infraestructura en la situación de estudio.

k) Nivel de Riesgo Residual

Nivel de riesgo que persiste una vez considerados los controles o medidas de seguridad para paliar los riesgos, determinando de esta forma la eficacia de las medidas implementadas.

l) Sabotaje

Destrucción, daño, o manipulación que se hace intencionadamente en una infraestructura, instalación, servicio, proceso, etc., con la intención de causar un serio perjuicio, alarma social, miedo, desprestigio, etc., como forma de lucha o protesta en conflictos políticos, sociales, laborales, económicos, contra la organización (organismo o empresa) que la dirige, o bien como método para beneficiar a una persona o grupo.

Tipos de Sabotaje:

- **Físico**. Destrucción, manipulación o alteración de los componentes de una infraestructura o sus instalaciones, que produce daños directa o indirectamente en la infraestructura, los trabajadores o la sociedad.
  Este sabotaje está castigado en el Código Penal. L.O. 10/1995, de 23 de noviembre, artículos 263, y 265:" daños a bienes de dominio o uso público o comunal, arruinen al perjudicado o se le coloque en grave situación económica, empleo de sustancias venenosas o corrosivas, infección o contagio de ganado".
  El artículo 346 del Código Penal, es aún más explícito para las infraestructuras: "destrucción de aeropuertos, puertos, estaciones, edificios, locales públicos, depósitos que contengan materiales inflamables o explosivos, vías de comunicación, medios de transporte colectivos, o la inmersión o varamiento de nave, inundación, explosión de una mina o instalación industrial, levantamiento de los carriles de una vía férrea, voladura de puente, destrozo de calzada pública, daño a oleoductos, perturbación grave de medio de comunicación, perturbación o interrupción del suministro de agua, electricidad, hidrocarburos".
- **Cibernético**. conductas dirigidas a eliminar o modificar funciones o datos en una aplicación informática sin autorización, para tomar control no autorizado del dispositivo, obstaculizar su correcto funcionamiento, obtener información, causar daños en el hardware o en el software del sistema, etc.
  Estos actos son punibles según estipula el Código Penal. L.O. 10/1995, de 23 de noviembre, artículo 264: "cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".
- **Informativo o reputacional**: propaganda de descrédito hacia una persona, organización u institución con la intención de dañar su imagen. En el ámbito privado se dispone del derecho a la protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (ley Orgánica 1/1982, de 5 de mayo), y en el ámbito empresarial se denomina Competencia Desleal y está penalizado por el artículo 38 de la Constitución. En el ámbito público, sin embargo, no está penado, en España no existe el delito de "alarma social".
  Dentro de este sabotaje estarían las denominadas "campañas de desinformación", principalmente a través de las redes y prensa digitales, donde creando "noticias falsas" con apariencia verosímil, o difundiendo opiniones que convierten en hechos probados, los difunden viralmente en la red, manipulando la realidad, o redireccionando las opiniones. Cuando llega a las redes el posible desmentido, los atacantes ya han conseguido crear el clima propicio para sus objetivos.
- **Sanitario**. es el acto no autorizado, donde se busca y pretende, dañar o destruir, instalaciones o servicios sanitarios de origen público o privado, y la contaminación del aire, agua, o sustancias, la alteración o manipulación de medicamentos, productos de alimentación con fines ilícitos.
  Está penado en el Código Penal. L.O. 10/1995, de 23 de noviembre, artículos 359 y siguientes: "quien elabore sustancias nocivas para la salud o productos químicos, medicamentos, alimentos que puedan causar estragos, o los despache o suministre, o comercie con ellos, etc.".

- **Social**: acto de sabotaje en el que se ve involucrado un grupo multitudinario de personas para cumplir una reivindicación no legalizada.
- **Terrorista**. Amenaza o actuación indiscriminada proveniente de un grupo organizado con la intención principal de infundir terror, a través de coacción, intimidación, daño o sometimiento a riesgo de personas, propiedades, o infraestructuras.
- **Bélico**. Actuaciones violentas de una nación contra otra realizadas por fuerzas militares.

3 CASOS HISTÓRICOS

Aunque los sabotajes en el mundo del agua no han sido unos de los sectores más utilizados para la consecución de fines deshonestos, el futuro nos traerá una menor disponibilidad del recurso como consecuencia del incremento de población y del cambio climático, y seguramente un empeoramiento de su calidad, lo que potenciará sin duda, los actos malintencionados.

A continuación, se exponen algunos ejemplos de la utilización del sector del agua y en particular las presas, con fines violentos.

- Sabotaje Físico.

- Presa de Itoiz (Navarra, España 1996). Tras golpear y atar a un vigilante de seguridad, ocho saboteadores cortan los cables de acero del blondín de colocación del hormigón de la presa, causando pérdidas valoradas en más de 12 millones de euros de la época.

Ilustración 1. Sabotaje de los cables del blondín de la presa de Itoiz (Navarra).

- Presa de Hat Gyi (Birmania, 2005). Un grupo no identificado asesina a un ingeniero tailandés durante la construcción de la presa en el río Salween del estado de Karen.
- Presa de Elche (Alicante, España 2008). Unos desconocidos abren la compuerta del desagüe de fondo provocando el vaciado de un millón de metros cúbicos de agua y lodo del embalse.
- Central hidroeléctrica de Baksan (Rusia, 2010). Hombres armados matan a dos trabajadores de una central hidroeléctrica y vuelan sus dos turbinas

- Cibernético. En el año 2019, el Centro Criptológico Nacional (CCN) y el Instituto Nacional de Ciberseguridad (Incibe), contabilizaron más de 150.000 incidentes de ciberseguridad a empresas, particulares y centros académicos. A continuación, se reproducen algunos ciberataques en el sector del agua:

- Año 2000. Maroochy (Australia). Un antiguo empleado despedido por su compañía utiliza su conocimiento para acceder a los sistemas de una planta de tratamiento de agua residual y realizar un vertido de agua sin tratar.
- Año 2011. Springfield (Illinois, EEUU). Un atacante que actúa desde una dirección IP situada en Rusia accede al sistema SCADA de una planta de tratamiento de aguas de la ciudad y realiza acciones que termina con la destrucción de una de las bombas de impulsión de la infraestructura. (Primer ciberataque confirmado contra una infraestructura crítica estadounidense).
- Año 2013. Hackers iranís se infiltran en el sistema de control de una presa situada a sólo 25 millas de la ciudad de Nueva York, convenciendo a la Casa Blanca para doblar esfuerzos para acelerar las defensas de Estados Unidos contra ataques cibernéticos.
- Año 2016. Se produce un acceso ilícito a los SCADAS del Canal de Navarra (Navarra, España) y se difunde por internet.

- Informativo. Como ejemplos se podrían incluir las “Campañas de desinformación”, las interferencias o manipulaciones en las elecciones de Estados Unidos de 2016, elecciones del Brexit de 2016, o la crisis catalana de 2017. También información periodística sensacionalista, por ejemplo “Pesticida en el agua aragonesa, el Chernobil español”, o “La rotura de la presa de Yesa sumergiría media Zaragoza bajo 7 metros de agua” (España, 2016).

- Social

- Año 2020. Agricultores mexicanos emboscan a cientos de soldados estatales que custodiaban la presa La Boquilla en Chihuahua (México), en medio de una disputa por el agua en la frontera con Estados Unidos. El gobierno mexicano estaba enviando agua a Texas cumpliendo el tratado internacional y según los agricultores dejaba casi sin nada para sus cosechas. Los asaltantes tomaron la central hidroeléctrica causando daños valorados en 4 millones de euros que tardaron tres meses en ser reparados e impidieron el flujo de agua hacia Estados Unidos.

- Sanitario.

- Año 1972. El Grupo Neo Nazi «Orden del Sol naciente» intenta envenenar el agua de Chicago, San Luis, y otras ciudades del medio oeste americano, con bacterias de Tifus, atacando los sistemas de distribución.

- Año 1973. Un biólogo alemán intenta lo mismo con ántrax y toxinas botulínicas a cambio de 8 M$.
- Año 1983. Intento de envenenamiento del agua de Galilea.
- Año 1985. El grupo extremista «El Convento, la espada y el brazo del señor (CSA)» intenta el envenenamiento de los sistemas de distribución de agua de Nueva York, Chicago y Washington, con cianuro de potasio.
- Año 1992. Concentraciones letales de cianuro de potasio se detectan en los depósitos de almacenamiento de agua de una base aérea en Estambul (PKK, Partido de los trabajadores del Kurdistán).
- Año Cuatro hombres arrestados en Roma en posesión de productos químicos y mapas detallados de la red de abastecimiento del Área de la Embajada de Estados Unidos.
- Año 2002, EEUU. Dos agentes de Al Queda arrestados en Denver con planes para envenenar los suministros de agua.
- Año 2004, EEUU. El FBI y el Departamento de Seguridad Nacional señalan que los terroristas estaban tratando de reclutar trabajadores de plantas de agua.
- Año 2006, Inglaterra. Un tanque de agua en Tring (Inglaterra) fue contaminado con herbicida.
- Año 2006, Dinamarca. En un embalse danés se vierte estricnina.
- Año 2007, China. Mueren 201 personas cuando se utilizó agua contaminada con fluoraetamida.
- Año 2008, EEUU. En Varney (Virginia) un hombre fue detenido con 2 frascos de cianuro para envenenar el suministro de agua.
- Año 2008, Tailandia. El suministro de agua de un campo de refugiados en Tailandia, con una población de 30.000 personas, fue envenenado intencionalmente con herbicida.
- Año 2009, Filipinas. El Frente Moro de Liberación Islámica (MILF) de Filipinas envenenó fuentes de agua que estaban siendo utilizadas por los soldados del gobierno y la población.
- Año 2010, India. En la región de Cachemira (India) los rebeldes maoístas envenenaron un estanque utilizado como fuente de agua potable por la Central Reserve Police Force, un grupo paramilitar.
- Año 2010, Inglaterra. Una pareja de neonazis fue declarada culpable de la fabricación de ricina y de conspiración para envenenar los suministros de agua utilizados por musulmanes.
- Año 2011, España. En la Línea de la Concepción (Cádiz) se descubrió un complot para envenenar los suministros de agua en respuesta a la muerte de Osama Bin Laden.
- Año 2012, Australia. Dos tanques de agua potable de 5.000 litros fueron envenenados deliberadamente en Diuron.
- Año 2012, Afganistán. Enferman cientos de niñas de una escuela cuando el suministro de agua fue envenenado intencionalmente.
- Año 2020, China. El coronavirus con millones de infectados se ha convertido en una pandemia a nivel mundial. Aunque su transmisión no es por el agua, sí que ha servido para cuantificar los efectos y consecuencias.

  - Terrorista.
- Panauti Plant y Seleghat Dam (Nepal 2001 y 2004). Grupos disidentes maoístas vuelan dos centrales hidroeléctricas.
- Presa de Kajaki (Afganistán, 2003 y 2008). El grupo terrorista ISIS lanza tres cohetes y explosivos a la presa y mata a 11 soldados ingleses.
- Presa de Haditha (Irak, 2015). Terroristas del grupo ISIS lanzan 7 coches bomba a la presa de Haditha pereciendo 20 atacantes.

Ilustración 2. Fotografía de la presa de Haditha

- Pakistán, 2015. Al menos 20 trabajadores son asesinados por un grupo separatista por trabajar en la construcción de una presa respaldada por el ejército en la provincia de Balochistán, en el sudoeste de Pakistán.
- Presa de Mosul (Irak, 2016). Las tropas italianas bajo mandato de la ONU, vigilan la presa de Mosul (Irak) que se encuentra en peligro después de una amenaza "específica y detallada" de un ataque de militantes de ISIS. Dijeron que el ataque sería "el mayor jamás concebido por el Califato" en Irak. Será "un asalto a gran escala que han estado trabajando durante meses".
- Presa de Salma (Afganistán, 2017). Los talibanes matan a 10 vigilantes de seguridad.

Ilustración 3. Fotografía de la Presa de Salma (Afganistan)

- Bélico. Es con mucho del que se tienen más datos.

- Durante la Guerra Civil Española (1936-1939) se afectaron, al menos, las siguientes presas:
  - Pena (Teruel). Las tropas republicanas volaron los Desagües de Fondo, rompiendo las compuertas de seguridad y regulación y vaciando bruscamente la presa.
  - Santolea (Teruel). Las tropas republicanas volaron las compuertas de regulación del desagüe de fondo sin afectar a las de seguridad. También volaron el puente del aliviadero.
  - Barasona (Huesca). Las tropas golpistas querían volar el desagüe de fondo, pero el Encargado les convenció de que era más sencillo abrir las compuertas del desagüe y así lo hicieron.
  - Ordunte (Burgos). Las tropas republicanas intentaron, sin éxito, volarla explosionando 2.500 kilos de dinamita en coronación.

- En la Segunda Guerra Mundial se encuentran los casos más numerosos:
  - Dnieprostroi (Rusia, 1941). El Ejército Rojo hizo una brecha de 10m x 120m colocando 20 tn de amonal, en la presa hidroeléctrica, produciendo una onda de avenida que se extendió desde Zaporizhia a Nikopol, matando a los residentes locales, así como los soldados de ambos lados. El número de víctimas, lo sitúan los historiadores entre 20.000 y 100.000.

Ilustración 4. Fotografía de la brecha en la presa de Dnieprostroi (Rusia, 1941).

  - Dnieper (Rusia, 1941) las tropas del Ejército Rojo en retirada demuelen con dinamita la presa y la central hidroeléctrica estratégica después de la invasión alemana de la Unión Soviética

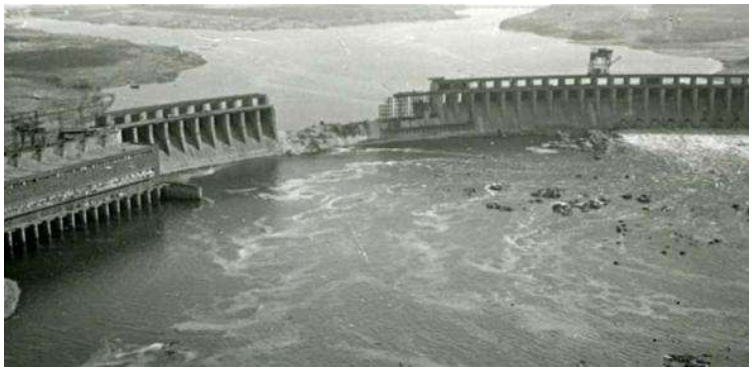

Ilustración 5. Brecha en la presa de Dnieper (Rusia, 1941).

- Dambusters Durante la Segunda Guerra Mundial, el ejército inglés ideó un plan de demolición de las presas alemanas (Möhne, Eder, Sörpe) y mediante bombas de rebote que se desplazaban sobre la superficie del agua del embalse. En otras se intentó como Ennepe pero no se consiguió. Se denominaban Dambusters, 16 bombarderos Lancaster del Squadron 617 creados específicamente para destruir el centro industrial alemán (la energía, las fábricas del Ruhr y las infraestructuras de ferroviarias).

Ilustración 6. Presa de Möhne (Alemania, 1943). Esta presa contaba con antiaérea y fueron necesarios cuatro ataques para su demolición

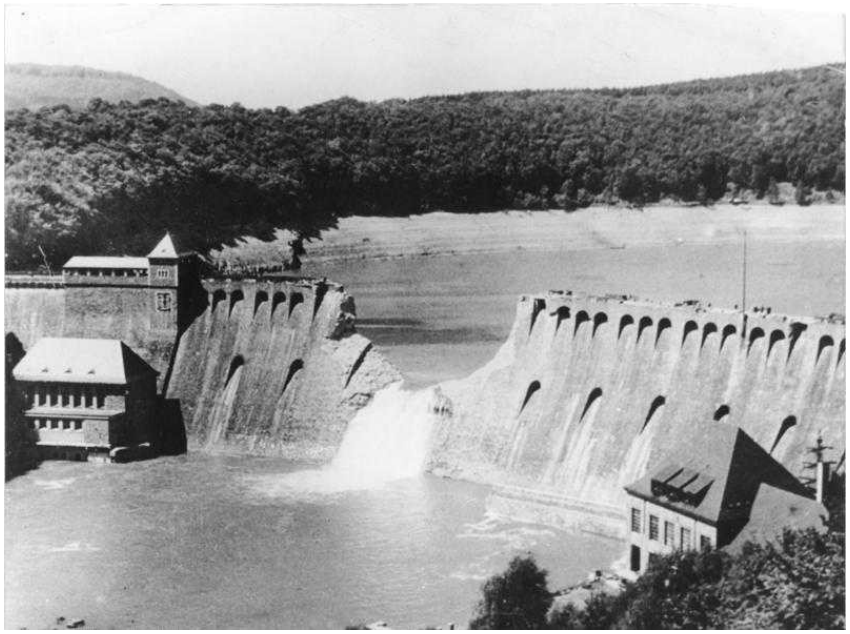

Ilustración 7. Presa de Eder (Alemania. 1943). El 15 de mayo de 1943 se produjo el ataque inglés, pero a pesar de la falta de defensas antiaéreas, no fue nada fácil por su complicada topografía con un fuerte encajamiento de la presa, necesitando tres intentos para su para su rotura

Ilustración 8. . Presa de Sörpe (Alemania. 1943). A pesar de los hundimientos con forma de cráter que se observan en la presa de materiales sueltos, ésta no se brechificó debido a las defensas antiaéreas, la complicada topografía y la niebla.

- Durante la guerra de Corea
    - Hwachon (Corea Sur, 1951). La presa de gravedad de hormigón de altura 78 m y 435 m de longitud de coronación, que fue construida por Japón

durante la Segunda Guerra Mundial. El 1 de mayo de 1951 el Grupo Aéreo 19 de USA bombardeó la presa desde ocho aviones Skyraiders, lanzaron 7 torpedos MK13, de los cuales explotaron seis, produciendo la rotura de dos compuertas, y dañando la tercera.

Ilustración 9. Presa de Hwachon (Corea Sur, 1951).

- Sui-ho (Corea del Sur, 1952). El Complejo Suiho, fue construido por los japoneses en 1940 en la Segunda Guerra Mundial. Tenía las seis turbinas más grandes del mundo de 100.000 KW y la capacidad de embalse era de 20 hm3. Era la principal fuente de alimentación eléctrica para las bases soviéticas en Port Arthur y Dalian (actual China), y al puerto ruso de Vladivostok en Siberia. El 24 de junio de 1952, el ejército americano atacó las centrales eléctricas y transformadores en la base de la presa.

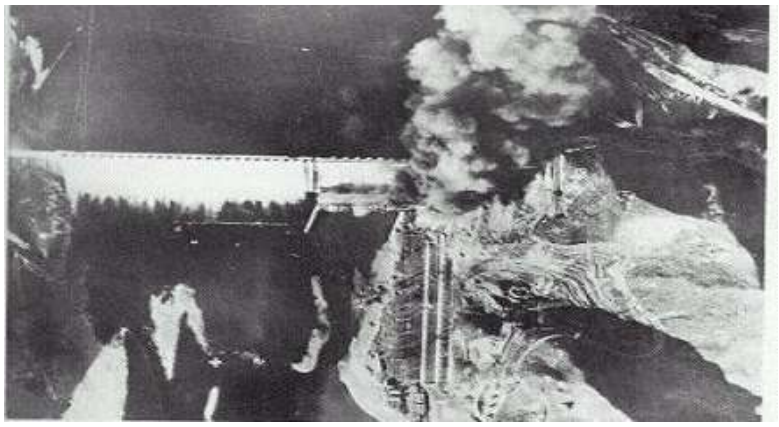

Ilustración 10. Presa de Sui-ho (Corea del Sur, 1952).

- Guerra de los Balcanes
    - Presa de Peruça (Croacia, 1993). Presa de materiales sueltos de 425 m de longitud de coronación y 60 m de altura construida entre 1955 y 1960. Fuerzas serbias, colocaron de 20 a 30 toneladas de TNT en cinco ubicaciones en el aliviadero y la galería de inspección, que no fueron suficientes para producir el fallo de la presa.

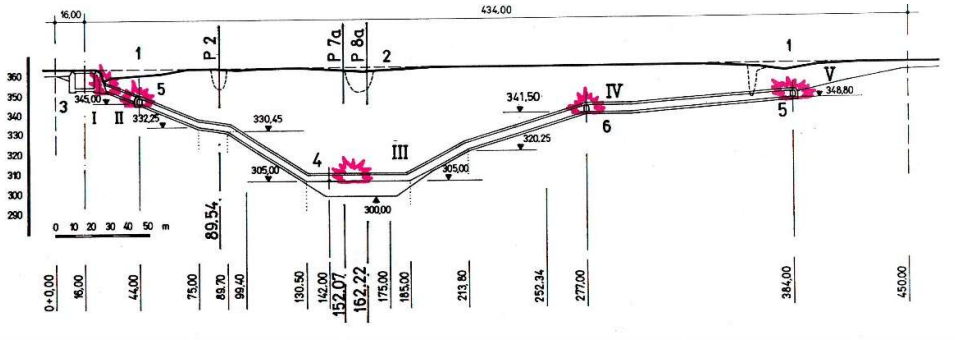

Ilustración 11. Colocación de explosivos en la presa de Peruca (Croacia).

Ilustración 12. Fotografía de los efectos de los explosivos en coronación de presa y aliviadero de Peruca (Croacia).

- Guerra de Ucrania
    - En junio de 2023, la presa ucraniana de Kajovka fue destruida por Rusia, lo que trajo consecuencias humanitarias y medioambientales importantes. La rotura de la presa provocó una subida del nivel del agua de hasta 5 metros en la región de Jersón, inundando al menos 30 poblaciones, afectando a unas 42.000 personas y siendo evacuadas unas 2.500 personas en la orilla bajo control ucraniano.

Ilustración 13. Vista de la destrucción de la presa ucraniana de Kajovka.

4 PELIGROS O AMENAZAS SOBRE LA INFRAESTRUCTURA

Como se ha descrito con antelación, en el marco de la presente guía, peligrosidad, peligro, amenaza tienen un mismo significado. Se descartan los fallos de seguridad estructural de la infraestructura por exceder de los límites de esta Guía.

En el Anexo Nº 1 se presenta una ampliación de las Amenazas

Se establecen dos divisiones: Amenazas globales que pueden afectar a cualquier Infraestructura y Particulares que sólo afectan a las presas y embalses, o lo hacen de una manera diferente:

A. AMENAZAS GLOBALES

1. Riesgos meteorológicos
   - Avenidas e Inundaciones
   - Incendios
   - Tormenta eléctrica
   - Contaminación electromagnética
   - Huracanes y tornados
   - Ola de calor
   - Ola de frío
   - Sequía extrema
   - Hielo, nieve extremos

2. Riesgos Geofísicos
   - Terremotos
   - Deslizamientos
   - Hundimientos o dolinas
   - Erupciones volcánicas
   - Tormenta geomagnética

3. Terrorismo y crimen organizado
   - Explosivos en personas suicidas
   - Explosivos en vehículos terrestres tripulados
   - Explosivos en vehículos terrestres no tripulados
   - Explosivos en aeronaves no tripuladas
   - Explosivos en lanchas o botes no tripulados
   - Explosivos en lanchas o botes tripulados
   - Explosivos en vehículos parados
   - Explosivos en paquetes enviados por correo

- Explosivos colocados o abandonados
- Ataques con lanzagranadas/morteros
- Ataque terrorista armado
- Envenenamiento masivo
- Ataque químico
- Ataque radiológico
- Ataque biológico
- Ataque nuclear
- Incendio intencionado
- Pulso electromagnético

4. Crímenes agresivos
   - Agresión y extorsión
   - Sabotaje
   - Amenaza de bomba

5. Delincuencia ordinaria
   - Robo
   - Hurto
   - Fraude
   - Vandalismo
   - Ocupación Indebida

6. Cibernéticos

B. AMENAZAS PARTICULARES

1. Fallo Físico Malintencionado
   - Corte de accesos físicos a la infraestructura.
   - Corte malintencionado de energía de red, telefonía, comunicaciones, etc.
   - Intrusión en instalaciones impidiendo el control de las mismas.
   - Accionamiento malintencionado de compuertas (aliviaderos, desagües de fondo o tomas) o rotura de conductos.
   - Obstrucción o introducción de elementos extraños en los conductos de aireación de válvulas y compuertas, bocas de hombre de tuberías, etc.
   - Destrucción de cuadros de accionamiento de compuertas.
   - Voladura o deterioro grave de elementos de la presa.
   - Manipulación del drenaje en presas de fábrica
   - Contaminación intencionada del agua embalsada, o redes de suministro.
   - Contaminación intencionada del aire de galerías o cámaras.
   - Utilización de drones con explosivos o contaminantes.
   - Sabotaje intencionado por personal propio de la organización

- Ataques dirigidos (suplantación, abusos, repudio, destrucción etc.)

2. Fallo de sistemas ciberfísicos
   - Interferencia en el software de supervisión que resulte en la imposibilidad de visualizar el estado actual o actuar a través de las interfaces hombre-máquina del sistema: Cifrado de servidores de tiempo real, acceso no autorizado a interfaces de supervisión o gestión…
   - Interferencia en la electrónica de red y comunicaciones que resulte, por ejemplo, en la pérdida de comunicaciones: modificación de la configuración de red, etc.
   - Interferencia en las comunicaciones con el propósito, por ejemplo, de representar valores falsos (cotas de lámina de agua, posición de compuertas…): ataques de tipo MITM (Man-in-the-Middle), etc.
   - Interferencia en el nivel de control (acciones sobre controladores, PLC, remotas, etc.) con el propósito de alterar el funcionamiento normal del sistema: realización de operaciones indebidas, funcionamiento del sistema impredecible, falseo de la información recibida por los operadores, activación/inhibición de alarmas…
   - Interferencia en la instrumentación (manipulación de datos para provocar maniobras erróneas).
   - Interferencia en los actuadores con el fin de realizar operaciones indebidas o, alternativamente, impedir maniobras (modificación de configuraciones, órdenes de marcha/paro de bombas, de apertura/cierre de compuertas, etc)

A continuación, se hace una descripción detallada de las amenazas más vulnerables, que pueden dar lugar a importantes modos de fallo en una presa y otras instalaciones hidráulicas.

4.1 Fallo del control de accesos.

4.1.1 Introducción

El control de accesos es el conjunto de dispositivos a implantar para el control, comprobación, identificación, inspección, intervención o fiscalización del paso o circulación de personas, vehículos u objetos a una zona o recinto previamente definido como área de control o de seguridad para la prevención y protección ante riesgos que puedan afectar a personas, bienes y/o instalaciones[1].

El control de accesos se puede aplicar tanto a personas como a vehículos o a materiales y objetos. Asimismo, este control puede ser autónomo o centralizado y utilizar medios técnicos físicos, mecánicos o electrónicos, usándose normalmente una combinación de los tres.

Los principales sistemas de control de accesos son los siguientes:

- Control de acceso peatonal: credencial material, credencial de conocimiento o credencial personal
- Control de acceso vehicular: control de matrículas, contraste con un código, comprobación de horario y conductor.
- Control de acceso de materiales y objetos: explosivos, armas, artefactos explosivos, otros.

La situación de crisis sanitaria derivada de la pandemia de COVID-19 ha introducido además una nueva variable en el control de accesos, que es evitar la propagación de la epidemia. En base a esta necesidad se han introducido nuevas herramientas en el control de accesos como es el caso de sensores para detectar que el personal accede con mascarilla o dispositivos de control de la temperatura corporal.

4.1.2 Modos de fallo

El control de accesos falla en el momento que cualquier persona vehículo u objeto no autorizado entra en las instalaciones burlando el sistema de control de accesos. Este fallo puede ser la puerta a amenazas de todo tipo, pudiendo provocar tanto daños físicos como lógicos en la estructura.

Se pueden identificar, entre otros, los siguientes modos de fallo en el control de accesos:

- Fallo por acceso no detectado.
- Fallo por acceso no autorizado mediante suplantación de identidad.

---

[1] Definición tomada del *"Manual para el Director de Seguridad"*. Manuel Sánchez Gómez-Merelo. E.T. Estudios Técnicos, SA. 1996.

Se puede considerar asimismo el acceso mediante el uso de métodos violentos o expeditivos, si bien no es un fallo del sistema de control de acceso como tal, sino el fallo de los sistemas de seguridad pasiva.

Aunque no sea objeto de este apartado, conviene incidir en la necesidad de complementar el sistema de control de accesos con otros sistemas de protección de las instalaciones como son:

- Sistemas de protección física perimetral e interior de las instalaciones.
- Sistemas de televigilancia.
- Sistema de coordinación con el centro de seguridad corporativo y con los centros operativos de las fuerzas y cuerpos de seguridad.

4.2 Corte de acceso físico.

4.2.1 Introducción

El corte de los accesos físicos a la presa limita las acciones de protección y auto-protección de la organización.

El corte del acceso no es por sí mismo un elemento de riesgo para la seguridad de las presas, pero **en el caso de un sabotaje es una acción previa para alargar el tiempo de reacción** y proporcionar al atacante un periodo adicional para acometer acciones de mayor calado sobre la presa y sus instalaciones.

4.2.2 Factores que influyen en el corte

Las presas se encuentran en lugares con accesos muy diversos. Algunas se ubican próximas a carreteras de la red pública y cerca de poblaciones y tienen tráfico más o menos frecuente. En dichas infraestructuras es más difícil la realización de actos de sabotaje.

Sin embargo, muchas otras presas se sitúan en lugares aislados en los que el camino de acceso es una derivación propia hacia la presa y están poco transitados, en estos casos es más sencilla la realización del corte del acceso.

El corte del acceso puede hacerse disponiendo algún elemento que bloquee la carretera (rocas de grandes dimensiones, árboles, cadenas, etc.) o destruyendo un tramo de la misma.

Entre estas acciones, el bloqueo es una acción relativamente sencilla de llevar acabo ya que no precisa de medios especiales, es por tanto la que debe considerarse como más probable.

El corte de un tramo de la carretera, requiere el uso de medios de mayor envergadura como maquinaria de obras públicas o explosivos y es, por tanto, más complejo de articular.

4.2.3 Normativa en relación a los accesos

La Norma Técnica de Seguridad para el proyecto, construcción y puesta en carga de presas y llenado de embalses, aprobada por Real Decreto 264/2021 de 13 de abril, se indica que: "*la presa y sus instalaciones estarán dotadas de accesos garantizados, incluso en circunstancias adversas, salvo justificación específica"* (art 19.1).

En el Reglamento Técnico de Seguridad de Presas y Embalses (RTSPE) se recomienda que *la presa disponga de accesos alternativos para permitir su comunicación en casos extremos* (art. 22).

La Instrucción de Grandes Presas indica también de manera genérica que se considerarán los accesos para construcción y conservación de la presa (art 23).

La Directriz básica de protección civil ante el riesgo de inundaciones no concreta nada en relación los accesos. Si bien, en la implantación de los Planes de Emergencia es habitual que se habiliten varios accesos a la presa y Sala de Emergencia (principal y alternativo).

Aunque las presas dispongan de diferentes accesos debe contemplarse que el acceso principal suele ser el más directo y la vía de acceso habitual y que la entrada por el acceso alternativo, una vez descubierto el corte en el principal, no será inmediata. Ello debe tenerse en cuenta de cara a la estimación de los tiempos de reacción en caso de sabotaje.

4.2.4 Tratamiento en los Planes de Emergencia

En los Planes de Emergencia de presas el corte de los accesos se ha catalogado tradicionalmente como un indicador de "*dificultad de actuaciones*", por lo que no se suele disponer de procedimientos específicos para su tratamiento. Ello es debido a que en los planes no se relaciona el corte con un ataque posterior. Este hecho, no debe obviarse en el ámbito de las infraestructuras críticas o estratégicas y debe vincularse con la posibilidad de un sabotaje.

4.2.5 Evaluación de la gravedad del corte

Tal y como se ha indicado, el acceso será más vulnerable cuanto menos tráfico soporte y también cuanto más largo sea.

Las consecuencias del corte se pueden cuantificar en función del tiempo que permanecerá aislada la presa. Dependerá de la detección del incidente, del tipo de corte (bloqueo u destrucción de la vía) y del tiempo de respuesta de las Fuerzas de Seguridad del Estado.

En cuanto a la detección del incidente, esta puede no realizarse hasta el momento en que se encuentre el obstáculo en la carretera, por lo que es muy probable que antes se detecte otra acción ya en las instalaciones de la presa. Por ello, la posibilidad de corte en el acceso debe advertirse a las Fuerzas de Seguridad del Estado en cuanto se transmita la alarma de sabotaje.

4.2.6 Otros tipos de corte

También se pueden considerar en este apartado los cortes de electricidad, telefonía, líneas de transmisión de datos y comunicaciones en general, que pueden dejar la presa incomunicada e inoperativa, especialmente en aquellas que se gestionan desde centros de control centralizados. Los casos relacionados con la interferencia en las comunicaciones asociadas a la supervisión u operación remota se tratan en el punto 4.8 **Error! Reference source not found.**dedicado a ciberseguridad.

4.3 Ataque con drones.

4.3.1 Introducción

El dron, UAV (Unmanned Aerial Vehicle), o VANT (vehículo aéreo no tripulado), es un vehículo aéreo no tripulado capaz de mantener de manera autónoma un nivel de vuelo controlado y sostenido, y propulsado por un motor de explosión, eléctrico o de reacción.

El concepto de “no tripulado” puede dar lugar a confusión, porque, aunque en el interior del vehículo no va ningún tripulante, existe contacto entre el UAV y operadores en tierra, y puede estar ligado a personas en tierra, ya sean pilotos, controladores o cualquier otro tipo de operario relacionado con la monitorización de la aeronave. Con esta matización, no todo lo que está en el aire se considera un dron o UAV, ya que los globos aerostáticos o los misiles no son considerados como tales.

Los drones pueden estar controlados remotamente desde tierra por un operador, o pueden ser autónomos y seguir una trayectoria predefinida o un plan de vuelo programado. Hay pues dos estaciones que pueden manejar información del dron, la estación de tierra y la estación a bordo; dependiendo de cuan autónomo sea el dron la estación de tierra realizará más o menos funciones de forma habitual.

Su inicio y posterior desarrollo se debe a las necesidades militares que imperaron durante la Segunda Guerra Mundial y la posterior Guerra Fría. Un pequeño avión capaz de cruzar las líneas enemigas, tomar información e incluso alcanzar pequeños objetivos sin arriesgar la vida de ningún soldado. Posteriormente, este artilugio militar se ha transformado también en una herramienta útil para la sociedad civil, apareciendo los drones civiles y comerciales, utilizados en todo tipo de actividades: vigilancia de instalaciones, topografía, geografía, geología, agricultura, etc., e incluso para la lucha contra incendios o para operaciones de salvamento.

Los drones están en permanente avance e innovación, mejorando día a día sus prestaciones. Aparte del uso militar, los vehículos aéreos no tripulados son utilizados en un creciente número de aplicaciones civiles, sobre todo en labores que son demasiado "aburridas, sucias o peligrosas" para los aviones tripulados.

Dependiendo del objetivo con el que se diseñe, el UAV tendrá unas dimensiones y una tecnología apropiadas para llevar a cabo la tarea encomendada lo mejor posible. Debido a esto, los drones tienen una amplia variedad de formas, tamaños (desde varios metros de envergadura hasta unos pocos centímetros), configuraciones y características...

Los tipos básicos de drones son los siguientes:

- Según las alas:

  - Drones de alas fijas: poseen alas estáticas y son similares a un avión en su diseño y forma de vuelo.
  - Drones multirotor: tienen diversas hélices que giran en diferentes sentidos, y se pueden mantener en el mismo sitio o variar de posición.

- Según el control:

- Dron autónomo: no necesita de piloto que lo controle, se guía por sus propios sistemas y sensores.
- Dron controlado remotamente: el dron es pilotado directamente por un técnico mediante un dispositivo de control.
- Dron monitorizado: el dron dirige su propio plan de vuelo, y el técnico, aunque no puede controlar los mandos directamente, si puede decidir qué acción llevará a cabo.

- Según el tamaño:

- NANO-DRON, Nano-UAV o NAV (Nano Air Vehicles): Los nano-drones serán uno de los futuros componentes de los enjambres de drones.
- MICRO-DRON, Micro-UAV, MAV o µUAV: Capaces de ser lanzados a mano y operar en alcances hasta 30 km, en general tienen dimensiones no superiores a 15 cm.
- MINI-DRON, mini-UAV o MUAV: Son los UAV por debajo de 25 o 30 kg de masa, con alcances sobre 30 km.
- Drones Pequeños, UAV de Corto Alcance o Close-Range UAV: Utilizados en operaciones de alcance hasta 100 km. En este grupo se encontrarán el mayor abanico de sistemas y vehículos.
- Drones tácticos, TUAV- Medium Range, UAV-táctico o Tactical UAV: Alcances entre 100 y 300 km.
- MALE (Medium Altitude Long Endurance): Altitud de operación moderada, entre 5.000 y 15.000 metros, y elevada autonomía, de hasta 24 horas. Funciones similares a las anteriores. El alcance de su operación suele ser menor (alrededor de 500 km).
- HALE (High Altitude Long Endurance): Gran altitud, de más de 15.000 metros, y más de 24 horas de autonomía. Misiones globales de reconocimiento y de vigilancia.
- Y aparte, los UCAV y UCAR, que son sistemas dispuestos para armamento de combate.

	Masa max. (kg)	Alcances max. (km)	Altitud vuelo (m)
NANO	< 0,5	5	50
MICRO	1,0	30	200
MINI	20	30	1000
PEQUEÑO	150	100	8000
TÁCTICOS	1000	300	10000
MALE	8000	500	15000
HALE	20000	1000	25000

Tabla 1. Clasificación de los drones

Los drones a utilizar contra las infraestructuras críticas o estratégicas podrían ser de cualquiera de los tipos vistos anteriormente, tanto los de uso militar (en caso de conflicto bélico o grupos terroristas organizados) como los de uso civil, que suelen ser de menor tamaño y capacidad de carga (Micro-dron, mini-dron y drones pequeños).

Sin embargo, en esta guía, no se van a contemplan las situaciones de conflicto bélico, por lo cual, los siguientes apartados se van a referir únicamente a los drones de uso civil, de más fácil acceso para cualquier persona que quiera utilizarlos contra una infraestructura.

4.3.2 Legislación considerada

El sector de los drones ha sido objeto de un gran crecimiento en España en los últimos años, por lo que ha surgido la necesidad de establecer un nuevo marco jurídico que permita un mayor desarrollo en condiciones de seguridad de este sector, tecnológicamente puntero y emergente.

Por este motivo, se han aprobado los **Reales Decretos 1036/2017 y 517/2024**, donde se regulan las operaciones con drones, establece las condiciones que deben cumplir las organizaciones de diseño, fabricación y mantenimiento de este tipo de aeronaves, requisitos de formación para su pilotaje, medidas relativas al uso recreativo, esto es, no profesional, estableciendo una serie de limitaciones destinadas a garantizar la seguridad del espacio aéreo y la seguridad de los ciudadanos.

El Consejo de Ministros aprobó el Real Decreto 1036/2017, de 15 de diciembre, publicado en el BOE del viernes 29 de diciembre de 2017, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea.

Además, las condiciones ahora aprobadas se completan con el régimen general de la Ley 48/1960, de 21 de julio, sobre Navegación Aérea, y establecen las condiciones de operación con este tipo de aeronaves, y otras obligaciones.

La norma establece requisitos para que los operadores desarrollen actividades mediante el uso de estos aparatos de manera segura en entornos hasta ahora no permitidos, como edificios, reuniones de personas al aire libre o vuelos nocturnos. Se contemplan los distintos escenarios y requisitos en los que se podrán realizar operaciones aéreas especializadas, vuelos, actividades deportivas, recreativas, de competición o exhibición.

La nueva regulación permite también llevar a cabo operaciones en espacio aéreo controlado, pero para ello será necesario contar con requisitos específicos de formación y equipamiento, así como un estudio aeronáutico de seguridad coordinado con el proveedor de servicios de tránsito aéreo y la previa autorización de la Agencia Estatal de Seguridad Aérea (AESA).

Igualmente, el documento establece las condiciones que han de cumplir las organizaciones para el diseño, fabricación y mantenimiento de las aeronaves, y señala los requisitos de formación de los pilotos, en línea con los marcos normativos de otros países europeos.

El Real Decreto 517/2024 regula el uso de UAS sobre infraestructuras críticas estableciendo restricciones y condiciones específicas para proteger estas áreas. En particular se menciona, que el uso de UAS en zonas restringidas que incluyen infraestructuras críticas está sujeto a las prohibiciones y restricciones establecidas en normativas previas, como el Real Decreto 1180/2018. En este contexto, se especifica que:

- Las zonas restringidas para la protección medioambiental y las zonas restringidas al vuelo fotográfico tienen regulaciones específicas que limitan el uso de UAS en estas áreas.
- Las infraestructuras críticas, que pueden incluir instalaciones estratégicas y de seguridad, están sujetas a un control más estricto para evitar riesgos a la seguridad nacional y a la integridad de estas instalaciones (Artículo 37 del citado RD 517/2024).

Sobre seguridad ciudadana:

El R.D 1036/2017 incorpora una serie de disposiciones complementarias dado que el uso de las aeronaves no tripuladas puede afectar a la seguridad pública. En esa línea, la norma obliga a que se comunique previamente al Ministerio del Interior aquellas operaciones con estos aparatos que se desarrollen sobre aglomeraciones y zonas urbanas. Asimismo, reserva la capacidad de las autoridades para limitar la operación con drones por motivos de seguridad pública.

El R.D.1036/2017 desarrolla el marco normativo adoptado inicialmente mediante el Real Decreto-Ley 8/2014, que establecía unos requisitos mínimos para la operación con este tipo de aeronaves, pero no abarcaba toda la casuística de potenciales actividades que el sector ha venido planteando posteriormente.

Uso recreativo de drones:

Este real decreto contiene medidas relativas al uso recreativo de los drones, estableciendo una serie de limitaciones destinadas a garantizar la seguridad del espacio aéreo y la de la ciudadanía. Por norma general, dichos vuelos habrán de llevarse a cabo fuera de los entornos urbanos (a no ser que el dron sea de peso inferior a 250 gramos), de día, alejados a más de ocho kilómetros de los aeropuertos, manteniendo el dron siempre a la vista a un máximo de 120 metros del suelo, en condiciones meteorológicas adecuadas (sin niebla, sin lluvia y sin viento), en espacio aéreo controlado y sin poner en peligro a personas y bienes en tierra.

Los requisitos establecidos en el real decreto están sujetos a la supervisión y control de AESA y su incumplimiento constituye una infracción administrativa en el ámbito de la aviación civil conforme a lo previsto en la Ley 21/2003, de 7 de julio, de Seguridad Aérea.

4.3.3 Modos de fallo

Los drones de uso civil, en sí, no suponen una amenaza o peligro, es el uso de ellos como medio para acercarse a una infraestructura portando algún elemento peligroso lo que supone un riesgo. Estos elementos peligrosos pueden ser explosivos o contaminantes, cuyo posible efecto se desarrolla en los apartados correspondientes.

El uso malintencionado de los drones en un riesgo a tener en cuenta, por las siguientes razones:

- Los drones de uso civil que pueden adquirirse en tiendas, por internet, y también por piezas, y los precios son relativamente asequibles.
- Son de fácil manejo para cualquier usuario.
- Pueden transportar hasta 10-12 kg de cualquier sustancia o elemento.
- Se pueden programar para aterrizar en un sitio concreto o para sobrevolar una zona concreta.
- Pueden volar a velocidades hasta de 90 km/h los de mayor tamaño.
- La autonomía de vuelo depende de las baterías. De 20 minutos hasta 6 horas (dron con 6 baterías)
- Disponen de posicionamiento GPS. Con este sistema, el grado de precisión en el punto de aterrizaje y trayectoria de vuelo es del orden de 2 a 5 m.
- Con posicionamiento GPS corregido, el grado de precisión es centimétrico.

4.3.4 Referencias

- Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto.
- Real Decreto 517/2024, de 4 de junio, por el que se desarrolla el régimen jurídico para la utilización civil de sistemas de aeronaves no tripuladas (UAS), y se modifican diversas normas reglamentarias en materia de control a la importación de determinados productos respecto a las normas aplicables en materia de seguridad de los productos; demostraciones aéreas civiles; lucha contra incendios y búsqueda y salvamento y requisitos en materia de aeronavegabilidad y licencias para otras actividades aeronáuticas; matriculación de aeronaves civiles; compatibilidad electromagnética de los equipos eléctricos y electrónicos; Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea; y notificación de sucesos de la aviación civil.
- Reglamento de Ejecución (UE) 2019/947 consolidado que incluye los cambios del Reglamento de Ejecución (UE) 2020/639 y Reglamento de Ejecución (UE) 2020/746.
- Reglamento Delegado (UE) 2019/945 consolidado que incluye los cambios del Reglamento Delegado (UE) 2020/1058.

4.4 Sabotaje por personal propio de la organización.

4.4.1 Introducción

A la hora de pensar en los modos de fallo en una presa, el posible sabotaje por personal de la propia organización no es de los primeros que se vienen a la mente. Quizá sea porque es un mundo de empresas muy especializadas y, en general, de tradición.

Pero también hay que tener en cuenta que el personal propio es el que mejor conoce la instalación. Esto implica que tiene facilidad de movimiento y orientación en el interior de la presa. Algo que no es nada sencillo para alguien que no esté habituado a moverse por galerías e instalaciones de una presa. De hecho, al ser cada presa única, incluso para alguien que esté acostumbrado a moverse por este tipo de instalaciones, le puede resultar difícil y complicado hacerlo por una presa desconocida. Por ello, el conocimiento de la instalación que tiene el personal propio de la organización, es un elemento muy valioso en caso de pretender llevar a cabo un sabotaje.

Alguien de la organización que quiera causar un daño puede actuar por iniciativa propia (enfermedad mental, despecho a sus superiores o a la empresa, sobornos...) o coaccionado por terceros que estén interesados en el daño (p.ej.: mediante secuestro de un familiar, amenaza de muerte, etc.).

En organizaciones con mucho personal involucrado en la explotación de la presa es complicado que se promueva el sabotaje de forma individual. De modo que, para llevar a cabo sabotajes que afecten directamente a la obra civil (p.ej. voladuras de partes de la presa) debido a su envergadura se tendría que contar con la complicidad de un grupo de personas de la organización involucrada. Este caso es muy improbable en tiempos de paz, si bien no habría que descartarlo en ningún momento.

Hay que tener en cuenta que como personal de la organización también se consideran a las empresas contratistas (servicios contratados) y sus empleados. Este tipo de personal, al no pertenecer directamente a la organización, conlleva una mayor dificultad de control, debido a la falta de conocimiento de los empleados y a que los procedimientos con los que trabajan son propios de la empresa contratista.

Resulta de interés la referencia señalada en la Directiva UE CER 2557/2024 de próxima transposición, sobre la posibilidad de consultar/comprobar antecedentes de personal cualificado (artículo 14) que presta servicio en activos críticos y/o vitales de una infraestructura crítica/estratégica acorde con las normativas y procedimientos establecidos tanto a nivel nacional como de la Unión Europea.

4.4.2 Modos de fallo

Una vez enumerados los aspectos más importantes a tener en cuenta, veamos a continuación los posibles Modos de Fallo más representativos relacionados con el sabotaje por personal propio de la organización son los siguientes:

a. Accionamiento indebido de órganos de desagüe
b. Corte de suministro eléctrico por daños en equipos de la presa (transformadores, grupos electrógenos …)
c. Relacionado con el anterior, estaría la extracción y venta ilegal de cable eléctrico de cobre, bastante habitual en los últimos años.
d. Si se permite el término, se podría hablar también de un posible “sabotaje indirecto”, en referencia a la no transmisión intencionadamente de incidencias/incidentes graves que afecten a la seguridad de la presa.
e. Facilitador de ataque de terceros.

4.5 Accionamiento malintencionado de compuertas

4.5.1 Introducción

En general, una amenaza consistente en el accionamiento malintencionado de compuertas puede conllevar una o varias de las pérdidas de misión siguientes, entre otras:

- Pérdida de la función de control y laminación de avenidas.
- Pérdida de almacenamiento de agua.
- Pérdida de producción hidroeléctrica
- Corte en el abastecimiento urbano y riego.
- Pérdida de uso recreativo.

Además, pueden incluirse otros eventos como por ejemplo manipulación o rotura de otros órganos de desagüe, desagües de fondo, tomas, infraestructuras secundarias, etc., que conlleven también pérdida de misión o bien daños a la propia presa o aguas abajo.

4.5.2 Modos de fallo

A continuación, se enumeran los posibles modos de fallo que pueden derivarse por accionamiento malintencionado de compuertas, incluyendo:

- APERTURA DE COMPUERTAS DEL ALIVIADERO.
- BLOQUEO DE COMPUERTAS DEL ALIVIADERO (IMPOSIBILIDAD DE APERTURA).
- APERTURA DE DESAGÜES INTERMEDIOS.
- APERTURA DE DESAGÜE DE FONDO.
- APERTURA DE TOMAS DE ABASTECIMIENTO.
- APERTURA DE OTRAS TOMAS.

4.6 Voladura o deterioro grave de elementos de la presa.

4.6.1 Introducción

Existe una creciente preocupación por el posible resultado de un ataque con explosivos a una infraestructura hidráulica, una presa o sus instalaciones asociadas. Se conce la existencia de planes de atentado contra presas por parte de grupos terroristas o criminales, aunque los detalles, y en particular, el grado de éxito que pudieran haber tenido, no ha sido generalmente desvelado.

Presa/Embalse	País	Plan frustrado	Organización	Descripción
Samarra	Irak	2015	DAESH	500 kg de explosivo
Salma	Afganistán	2013	Talibanes	1.300 kg de explosivo
Falcom	US / México		Zetas	Desconocida
Chingaza	Colombia	2002	FARC	Desconocida
Lhokseumawe	Indonesia	2001	Separatistas	Dispositivo explosivo
Panauti Plant	Nepal	2001	Insurgentes comunistas	Dispositivo explosivo
Kidapawan	Filipinas	2003	Insurgentes islamistas	Lanzacohetes
Kajaki	Afganistán	2003	Insurgentes islamistas	Lanzacohetes
Dumarao	Filipinas	2004	Insurgentes comunistas	Dispositivo explosivo
Selaghat	Nepal	2004	Insurgentes comunistas-maoistas	Dispositivo explosivo
Mirani	Pakistán	2005	Desconocido	Dispositivo explosivo
Haditha	Iraq	2005	Desconocido	Dispositivo explosivo
Haditha	Iraq	2005	Insurgentes islamistas	Lanzacohetes
Kajaki	Iraq	2005	Insurgentes islamistas	Dispositivo explosivo
Hlaingbwe	Myanmar	2007	Separatistas	Dispositivo explosivo
Hlaingbwe	Myanmar	2007	Separatistas	Lanzagranadas
Waeng Station	Tailandia	2007	Separatistas islámicos	Dispositivo explosivo
Kajaki	Afganistán	2008	Insurgentes islámicos	Dispositivo explosivo
Tipaimukh	India	2008	Desconocido	Dispositivo explosivo
Mosul	Iraq	2009	Desconocido	Dispositivo explosivo
Balimela Power Station	India	2009	Insurgentes comunistas-maoístas	Dispositivo incendiario
Mytikyina	Myanmar	2010	Separatistas étnicos	Dispositivo explosivo
Thawt Yin Kha	Myanmar	2010	Separatistas étnicos	Dispositivo explosivo
Machlagho	Afganistán	2011	Desconocido	Dispositivo explosivo

Tabla 2. Actividades terroristas con explosivos en presas.

También son conocidos los ataques a presas ejecutados en situaciones de conflicto bélico. Los Convenios de Ginebra prohíben expresamente (desde 1977, con la enmienda Protocolo I) el ataque a las presas, pero la realidad es que tanto anterior como posteriormente, se han producido ataques de este tipo. Durante la II Guerra Mundial, los aliados, concretamente la Royal Air Force de Reino Unido, lanzaron un ataque sobre cuatro presas alemanas en el contexto de la operación Chastise. En las presas de Mönhe y Eder, ambas de gravedad, las bombas consiguieron formar una brecha y vaciar el embalse. En cambio, en la presa de Sörpe, de materiales sueltos, las bombas tan solo consiguieron formar algunos cráteres en el espaldón de aguas abajo, sin llegar a desarrollar ningún modo de fallo que pudiera comprometer la estabilidad de la presa. Más recientemente, durante la guerra de los Balcanes, el ejército serbio colocó varias toneladas de explosivos en la galería de la presa de Peruca (en Croacia). La explosión produjo un asiento en la coronación y cráteres en los estribos, pero no llegó a romper a presa.

Es improbable que un ataque terrorista pueda tener éxito, pero la existencia de estas amenazas preocupa a los responsables, dueños u operadores de presas. Además, aunque no lleguen a comprometer la estabilidad de la presa, los ataques pueden afectar a su servicio o dañar a las personas que se encuentren cerca de la zona donde se produzca el ataque. Por ello es muy importante determinar qué efecto pueden tener los explosivos sobre las presas a corto y largo plazo.

El problema de la resistencia estructural ante cargas explosivas ha sido objeto de investigación durante muchos años, especialmente dentro de la comunidad militar. Aunque gran parte de estos hallazgos son de uso restringido, existe también amplia información disponible que puede ser de utilidad para aquellos ingenieros que diseñan, construyen y operan este tipo de infraestructuras.

En el caso de edificios, el Eurocódigo EN 1991-1-7 hace referencia a cargas accidentales y explosiones, pero se centra sobre todo en acciones impulsivas como el impacto de camiones, trenes, barcos, helicópteros o cualquier otro vehículo en general. También considera explosiones de gas en espacios cerrados, pero no existe un marco general para el tratamiento de cargas explosivas externas. El CTE (Documento Básico SE-AE Acciones en la edificación) solo cita que, en edificios con usos tales como fábricas químicas, laboratorios o almacenes de materiales explosivos, se hará constar en el proyecto las acciones accidentales específicas consideradas, con indicación de su valor característico y su modelo.

4.6.2 Generalidades sobre explosivos

Los explosivos son mezclas de sustancias químicas con un cierto grado de inestabilidad en los enlaces atómicos de sus moléculas que, ante determinadas circunstancias o impulsos externos, propicia una reacción rápida de disociación y nuevo reagrupamiento de los átomos en formas más estables. Esta reacción, de tipo oxidación-reducción, se conoce con el nombre de detonación y origina gases a muy alta presión y temperatura, los cuales generan a su vez una onda de compresión que recorre el medio circundante.

De esta forma, la energía química contenida en el explosivo se transforma en la energía mecánica de esa onda de compresión, en un corto espacio de tiempo.

En función de la cinética química se distinguen; **combustiones** (reacciones químicas de oxidación en la que generalmente se desprende una gran cantidad de energía con una velocidad de reacción menor a 1 m/s y que se pueden observar a simple vista en forma de llama), **deflagraciones** (como las combustiones con llama, pero desarrollándose a una velocidad inferior a la velocidad con que se propagaría el sonido en el propio explosivo y con ondas de presión del orden de 10^3 atmósferas) y **detonaciones** (combustión supersónica – entre 1.500 y 9.000 m/s - que generan una onda de choque con altos gradientes de presión – 10^5 atmósferas - y temperatura). La composición y características del explosivo, ente otras variables, determinan la velocidad de detonación, así como las presiones de burbuja y detonación.

4.6.3 Características

Las características más relevantes de un explosivo son:

Potencia explosiva	Capacidad para quebrantar y proyectar los materiales (energía efectiva en la voladura). Depende fundamentalmente de la composición.
Velocidad de detonación	Velocidad a la que se produce la transformación del material explosivo en gases. Los explosivos que detonan lentamente funcionan mejor en materiales más blandos y producen fragmentaciones más gruesas, mientras que los de elevada velocidad de detonación producen fragmentaciones más intensas en materiales duros.
Densidad de encartuchado	Cuanto mayor es la densidad del explosivo, mayor es la concentración de carga. Depende también de la composición y el proceso de fabricación. La densidad relativa de los explosivos está comprendida normalmente entre 0,8 y 1,5 (por debajo de 1,1 funcionan mal sumergidos).
Resistencia al agua	Capacidad para, (en ausencia de cubierta especial), mantener las propiedades inalterables durante un periodo de tiempo en contacto con el agua. Las dinamitas gelatinosas, hidrogeles y emulsiones resisten perfectamente al contacto con agua, pero los productos pulverulentos y ANFOs no (debido al carácter soluble del nitrato amónico). No obstante, en determinadas condiciones y en forma de emulsión o disolución saturada, puede ofrecer buena resistencia al agua. Prácticamente todos los tipos de explosivos toleran una cierta humedad siempre que el tiempo de permanencia de explosivo en esas condiciones sea breve. En el caso de explosivos a granel como el ANFO esta resistencia se debe al enfundado de los mismos a la incorporación aditivos.
Sensibilidad	Energía que hay que trasmitirle (mediante un detonador, una onda expansiva, impacto o fricción) para que se produzca su iniciación y, a continuación, su detonación.

Tabla 3. Características de un explosivo.

4.6.4 Clasificación de explosivos industriales

Según la magnitud del impulso energético necesario para iniciar su detonación:

• *Sustancias explosivas primarias*: Son aquellas, que, debido a la debilidad de sus enlaces, resultan altamente sensibles e inestables. Una pequeña cantidad de estas sustancias es ya sensible a la ignición (pequeña masa crítica). Se utilizan en la fabricación de detonadores. Ejemplos: fulminato de mercurio, azida de plomo y trinitrorresorcinato de plomo.

El peróxido de acetona (triperóxido de triacetona, peroxiacetona, "*madre de Satán*", TATP) es un potente explosivo primario que ha atraído la atención de grupos terroristas ya que puede fabricarse con productos de uso doméstico. No obstante, es altamente sensible a la temperatura, fricción e impacto por lo que su manipulación es complicada.

• *Sustancias explosivas secundarias*: Son sustancias explosivas para cuya detonación se requiere, en comparación con las anteriores, una mayor cantidad de explosivo y un mayor impulso energético. Se utilizan como carga base de los detonadores, como cebos para iniciar explosivos de baja sensibilidad y también, en mayor o menor proporción, forman parte de la composición de muchos explosivos comerciales.

Entre este tipo de sustancias cabe mencionar la nitroglicerina, el nitroglicol, el trinitrotolueno, la pentrita y la nitrocelulosa.

• *Sustancias no explosivas susceptibles de detona*r ante un impulso energético suficientemente alto (por ejemplo, la detonación de otro explosivo). Principalmente el nitrato amónico (de amplio uso en la industria, ya que se usa generalmente como fertilizante) el cual, añadiéndole un elemento combustible que corrija su balance de oxígeno positivo, forma parte de la mayoría de los explosivos comerciales actuales. Es un producto prácticamente inerte (por lo que es muy seguro de manejar) que se sensibiliza añadiendo en torno a un 5 – 6 % en peso de gasoil y es muy barato. Sin embargo, es altamente higroscópico y soluble en agua, por lo que se insensibiliza llegando a imposibilitar su detonación. Tiene un calor de explosión de solo 380 cal/g (aproximadamente una cuarta parte del correspondiente a la nitroglicerina), pero si se le añade un combustible puede incrementarse hasta superar las 900 cal/g.

Las mezclas de estas y otras sustancias dan lugar a los explosivos industriales más habituales, como los que se muestran a continuación:

Explosivo industrial	Composición	Características
Dinamita pulverulenta	Básicamente nitrato amónico; un combustible y una cantidad próxima a un 10% de un sensibilizador, que puede ser nitroglicerina, trinitrotolueno (TNT) o una mezcla de ambos.	Baja potencia Densidad media/baja (de 1,0 a 1,2) Regular o mala resistencia al agua Velocidad de detonación de 2.000 a 4.000 m/s Poca sensibilidad al choque o a la fricción.

		Rocas de dureza media-baja sin presencia de agua.
Dinamita gelatinosa	Mayor contenido de nitroglicerina (o Nitroglicol) más una cierta cantidad de nitrocelulosa, que actúa como gelificante, formando una pasta gelatinosa.	Elevada potencia Alta densidad (de 1,4 a 1,5) Buena o excelente resistencia al agua. Alta velocidad de detonación (de 4.000 a 7.000 m/s) Cierta sensibilidad al choque o a la fricción. Recomendables en rocas de alta resitencia, incluso con presencia de agua.
ANFO	ANFO (Ammonium Nitrate + Fuel Oil), 94 % aproximadamente de nitrato amónico que actúa como oxidante y en torno a un 6 % de gasoil que actúa como combustible ALANFO (Aluminium + Ammonium Nitrate + Fuel Oil).	• Baja / media potencia. • Muy baja densidad (0,8). • Nula resistencia al agua, ya que el nitrato amónico es soluble y pierde su capacidad de detonar. • Baja velocidad de detonación (2.000 - 3.000 m/s). • Necesitan de otro explosivo (cordones detonantes, cebos de dinamita gelatinosa, cartuchos de hidrogel o multiplicadores).
Hidrogeles (slurries o papillas explosivas)	Un elemento oxidante (NH_4NO_3 o bien $NaNO_3$) y otro que actúa a la vez como sensibilizador y combustible, y que puede ser un explosivo (TNT), un metal (Al) o una sal orgánica (Nitrato de Monometilamina o Nitrato de Hexamina) junto con una cierta cantidad de agua. A esta mezcla se le suele añadir también un conjunto de sustancias espesantes, gelificantes y estabilizantes.	• Elevada potencia. • Densidad media/alta (1,2-1,3) • Excelente resistencia al agua • Velocidad de detonación de 3.500 a 4.500 m/s. • Menor sensibilidad a la fricción o al impacto. Gran seguridad en el manejo y el transporte.

Emulsiones	Una fase dispersa (pequeñas gotas de disolución de NH_4NO_3 o de $NaNO_3$ en agua) rodeada de una fina película de 10-4 mm de aceite mineral (fase continua). Es decir, están compuestos básicamente por nitrato amónico o nitrato sódico con un contenido en agua entre el 14 y el 20 %, un 4 % aproximadamente de gasoil y menores cantidades (1 – 2 %) de otros productos, entre los que se encuentran agentes emulsificantes (oleato o estearato de sodio), ceras para aumentar la consistencia y el tiempo de almacenamiento, aire o esferas huecas de vidrio y partículas de aluminio que aumentan igualmente su potencia y sensibilidad.	De todo aquello se deriva un explosivo en forma de pasta, capaz de ser bombeado o de ser encartuchado • Alta velocidad de detonación (4.500-5.500 m/s) • Excelente resistencia al agua. • Mucha menor sensibilidad al choque o a la fricción.
Mezclas de ANFO con emulsión	Desde una proporción 90/10, ANFOs pesados, hasta 50/50.	• Variable resistencia al agua. • Densidades entre 1,25 y 1,10 g/cm^3. • Encartuchado, o a granel.

Tabla 4. Clasificación de explosivos industriales.

4.6.5 Conclusiones

- La detonación produce una acción impulsiva (altas presiones durante intervalos del orden de milisegundos).
- Estas detonaciones pueden tener efectos nocivos localizados (formación de cráteres y brechas) o generales.
- Diferentes aspectos del explosivo (material, cantidad), del punto de detonación (distancia y ángulo de exposición), del material expuesto (hormigón, tierra, escollera) y las condiciones del entorno determinan la importancia de las acciones impulsivas y de las roturas localizas.
- Las acciones a su vez pueden desencadenar distintos modos de fallo, si bien la mayoría no parecen viables debido a la gran cantidad de explosivos que se requieren y al alto grado de sofisticación de la acción que necesitan.

4.6.6 Referencias

- [Afriyie 2014] Effects of explosions on embankment dams, G. A. Afriyie, Master Thesis, Carleton University Ottawa, Ontario, 2014.
- [Bernaola Alonso et al. 2013] Bernaola Alonso, José; Castilla Gómez, Jorge y Herrera Herbert, Juan (2013). Perforación y voladura de rocas en minería. Universidad Politécnica de Madrid.
- [Busch 2016] Understanding the Behavior of Embankment Dams Under Blast Loading, C. L. Busch, PhD Thesis, University of New Mexico, 2016.

- [EUR 26456 EN] Calculation of Blast Loads for Application to Structural Components. JCR TEchnical reports, 26456 EN, European Commission
- [FEMA 2003] Primer for Design of Commercial Buildings to MitigateTerrorist Attacks, FEMA 427, 2003.
- [FEMA 2011] Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, FEMA-426, 2011.
- [FM 3-34.214] Explosives and Demolitions FM 3-34.214 (FM 5-250), Department of the Army – US, 2007.
- [Friedlander 1946] Friedlander, F. G. (1946). The diffraction of sound pulses. I. Diffraction by a semi-infinite plate. *Proceedings of the Royal Society of London A, 186*, 322–344.
- [Homeland Security 2012] Worldwide Attacks Against Dams, A Historical Threat Resource for Owners and Operators, 2012
- [IGME] Manual de perforación y voladura de rocas. López Jimeno et al, IGME.
- [Jia 2016] Jia, J. S., Xu, Y., Hao, J. T. y Zhang, L. M., “Localizing and Quantifying Leakage through CFRDs”, Journal of Geotechnical and Geoenvironmental Engineering. Eng., 2016, 142(9).
- [Lampson 1946] Lampson, C.W., Explosions in Earth, Effects of Impact and Explosion, Office of Scientific Research and Development, 1946.
- [Nonveiller 1999] Nonveiller, E., J. Rupcic, and Z. Sever, "War Damages and Recon-struction of Peruca Dam", Journal of Geotechnical and Geoenvironmental Engineering, 125(4), 1999, 280-288.

4.7 Sabotaje del sistema de drenaje interno y externo.

A continuación, se analiza el potencial sabotaje del sistema de drenaje en presas de fábrica, donde tanto en el cuerpo de presa como en el cimiento, constituye un elemento esencial del mecanismo resistente. De manera general, dentro de las presas de fábrica se consideran tanto las construidas empleando hormigones, como mampostería, y entre los mecanismos resistentes se suelen diferenciar las presas de gravedad, que movilizan esencialmente el rozamiento en el contacto entre la presa y el cimiento, además de los mecanismos que incorporan un efecto arco, con curvatura simple o doble. En todos los casos, las presas de fábrica incorporan un sistema de drenaje que, por un lado, limita la generación de fuerzas de subpresión en el cimiento y, por otro, trata de mantener el cuerpo de presa libre de flujo.

4.7.1 Relación entre modos de fallo y el sabotaje del sistema de drenaje

Es sabido que por modo de fallo se considera cualquier situación o proceso existente en el sistema presa-embalse susceptible de provocar que éste último deje de proporcionar los usos previstos, y por mecanismo de fallo a una de las potenciales secuencias de eventos que puede dar como resultado un modo de fallo. En este sentido, el sabotaje o manipulación del sistema de drenaje en presas de fábrica no constituye en sí mismo un modo de fallo, sino que realmente se trata de un evento que puede formar parte de algún mecanismo de fallo.

En cualquier caso, el sabotaje del sistema de drenaje es un evento donde se concentra la acción antrópica malevolente, y que se combinaría con el resto de elementos del potencial mecanismo de fallo. En caso de resultar efectivo, la consecuencia directa de este evento, que podríamos denominar "*sabotaje del sistema de drenaje"* sería, por tanto, la presencia de líneas de flujo y su correspondiente potencial hidráulico, con un incremento de las presiones y las fuerzas de subpresión asociadas, tanto en el cimiento como en el cuerpo de presa.

Si se analizan las estadísticas históricas relacionadas con roturas de presas de fábrica, siempre aparecen las fuerzas de subpresión como una de las causas o elementos fundamentales del mecanismo de rotura.

En el caso del cimiento, las inestabilidades en las que la existencia de presiones que generan fuerzas de subpresión importantes no sólo deben considerarse en el contacto estricto entre el cuerpo de presa y el cimiento, sino también en planos o superficies más profundas. Por otra parte, existen diferencias según que puedan producirse despegues en el pie de aguas arriba, con la conocida formación de la grieta de tracción. Del mismo modo, las condiciones y naturaleza del macizo rocoso pueden influir en el mecanismo debido a la presencia de material más o menos fracturado, y la propia disposición de los estratos y familias de diaclasas pueden igualmente dar como resultado mecanismos diferentes, incluso movilizándose cuñas del terreno, como sucedió en la rotura de la presa de Malpasset (ICOLD 2018).

Ilustración 14. Estribo izquierdo de la presa de Malpasset después de la rotura, donde se puede apreciar un "diedro" en el cimiento con la mitad del macizo de gravedad caído. ICOLD TCDS, 2018

En el caso de las inestabilidades en el cimiento de presas de fábrica, la empresa hidroeléctrica BC Hydro elaboró en el año 1995 una interesante síntesis de mecanismos genéricos de deslizamiento o vuelco, diferenciando los siguientes:

1. Inestabilidad al superarse la resistencia a cortante a lo largo de una discontinuidad del cimiento o en las cercanías del contacto presa-cimiento, que sólo podría producirse en un cimiento extremadamente débil, con una excavación defectuosa o una ausencia de tratamiento de la cimentación.
2. Inestabilidad al desarrollarse un área sin compresiones (grieta de tracción) y dar lugar a una superación de la resistencia a cortante en el contacto presa-cimiento. Este mecanismo sí que puede desarrollarse en cualquier tipo de cimiento, incluso los de buena calidad.
3. Inestabilidad al superarse la resistencia a esfuerzo cortante a lo largo de una discontinuidad pseudo-planar del cimiento, que también es factible en cualquier cimiento.
4. Inestabilidad al superarse la resistencia a esfuerzo cortante a lo largo de una discontinuidad escalonada o desarrollada en varias superficies pseudo paralelas del cimiento. En este caso, si las superficies de discontinuidad se encuentran cercanas puede asumirse el desarrollo de una superficie envolvente de rotura, mientras que, si las superficies de discontinuidad se encuentran más separadas, hará falta un análisis más complejo.
5. Inestabilidad por superación de la resistencia a esfuerzo cortante en un macizo rocoso de cimiento muy fracturado o dañado. Este mecanismo de inestabilidad es poco frecuente, aunque puede considerarse en el caso de macizos rocosos con múltiples familias de diaclasas y fracturados, donde se puede ajustar una superficie de rotura planar envolvente.

6. Inestabilidad al superarse la resistencia a esfuerzo cortante a lo largo de una combinación de discontinuidades del cimiento (no pseudo paralelas como en el cuarto mecanismo). Este tipo de mecanismo puede simplificarse inicialmente como del tipo 3 o 4, aunque puede abordarse su análisis mediante métodos de equilibrio límite.
7. Inestabilidad por pandeo o vuelco de estratos pseudo verticales en el cimiento. Se trata de un mecanismo poco probable, pero que debería considerarse en macizos rocosos muy estratificados y diaclasados con una disposición casi vertical. Este mecanismo, de existir, suele combinarse con el segundo.
8. Inestabilidad al superarse la resistencia a esfuerzo cortante en varias superficies tridimensionales del macizo rocoso del cimiento, formándose un diedro o cuña inestable por la combinación de fallas, diaclasas o juntas. Este mecanismo es poco probable, pero es precisamente el que se desarrolló en la mencionada presa de Malpasset, y lógicamente requiere un análisis tri-dimensional.

Para el cuerpo de presa, la rotura histórica de la presa de Bouzey demostró de forma empírica la necesidad del drenaje, mediante la materialización de unas perforaciones que llamaran a las líneas de corriente del flujo que se produce desde el embalse, a través del esqueleto mineral del hormigón de las presas. Dicho flujo suele concentrarse en los extremos de los bloques de presa, donde resulta más difícil la compactación del hormigón y éste presenta una peor calidad. Las mencionadas perforaciones se sitúan empíricamente cercanas al paramento de aguas arriba de la presa, separadas entre sí unos 3 m y conectadas verticalmente a través de las galerías de la presa, que suelen separarse unos 30-35 m entre sí.

Otras referencias clásicas, como el viejo "*Manual del vigilante de la presa*" (MOP, 1969), recogen con distintas representaciones el papel e importancia del sistema de drenaje, tanto en el cuerpo de presa como el cimiento, y el propio Comité Nacional Español de Grandes Presas lo hace en varias de sus guías técnicas, como las editadas con los números 1, 2 y 6 (SPANCOLD, 2005, 2003, 1999)

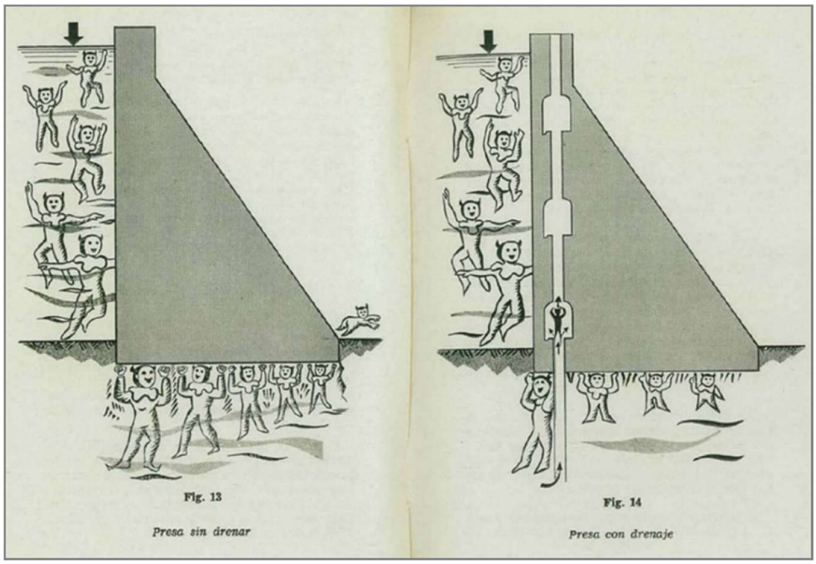

Ilustración 15. Importancia del drenaje en presas de gravedad. Fuente: Manual del vigilante de la presa. MOP, 1969

Las roturas de presas debido a fallos o problemas del sistema de drenaje en el cimiento, que dan lugar a un incremento patológico de las subpresiones o fuerzas inestabilizadoras que se desarrollan en la superficie de contacto entre la presa y el cimiento, o bien, en las interfaces entre estratos o las diaclasas del cimiento, constituyen un 17% de los casos históricos recopilados por varios autores a finales del siglo pasado. En la actualidad (año 2020), el ICOLD está actualizando su base de datos sobre incidentes y roturas de presas, pero en principio, puede esperarse que dicho porcentaje se mantenga cercano a esa cifra, que viene a implicar una quinta parte de las roturas.

Rango	Descripción	Nº	% de presas
Roturas			
1	Sobrevertido	10	22
2	Subpresión	8	17
3	Filtraciones en el cimiento	7	15
4	Erosión interna en el cimiento	6	13
5	Filtraciones excesivas	6	13
Accidentes			
1	Filtraciones en el cimiento	16	9
2	Erosión local/socavamiento	16	9
3	Erosión interna en el cimiento	13	7

4	Filtraciones excesivas	13	7
5	Fallo de los órganos de desagüe	10	6
Grandes reparaciones			
1	Ciclos hielo-deshielo	53	20
2	Gradientes de temperatura extremos	28	11
3	Reacciones evolutivas en el hormigón	22	8
4	Permeabilidad excesiva del hormigón	22	8
5	Reacciones evolutivas en la mampostería	22	8

Tabla 5. Causas principales de incidentes o roturas en presas de fábrica. Fuente: Douglas, Spannagle y Fell, 1998.

4.7.2 Conclusiones sobre el sabotaje de sistemas de drenaje

A partir de todo lo indicado respecto al sabotaje de los sistemas de drenaje en presas de fábrica, puede establecerse que la manipulación malevolente del sistema de drenaje constituye un evento que podría formar parte del mecanismo de varios modos de fallo. En general, los modos de fallo potenciales de una presa pueden desarrollarse en detalle con la ayuda de árboles de eventos o árboles de fallo.

La principal conclusión es que las probabilidades de poder generar un fallo masivo en una presa de fábrica mediante el manejo malintencionado del sistema de drenaje son muy reducidas. El sabotaje del drenaje implica la realización de una serie de tareas o actuaciones que resultan complicadas, incluso para alguien que tenga conocimiento de ingeniería de presas o esté familiarizado con las mismas. Por otra parte, esas actuaciones malevolentes tendrían un impacto limitado sobre la seguridad de la presa o su cimiento, aun contando con los medios necesarios para llevarlas a cabo y, sobre todo, con el tiempo necesario, dado que se trata de acciones con duraciones importantes.

4.7.3 Referencias

- Dam surveillance: Lessons learnt from case histories – ICOLD Bulletin Draft. Technical Committee on Dam Surveillance, ICOLD, Paris, France, 2018.
- Manual de empleo de explosivos. Dirección General de Política Energética y Minas, España, 2004.

- Guía Técnica de Seguridad de Presas Nº 1. Seguridad de presas. Comité Nacional Español de Grandes Presas y Colegio de Ingenieros de Caminos, Canales y Puertos, España, 2005.
- Guía Técnica de Seguridad de Presas Nº 2. Criterios para proyectos de presas y sus obras anejas (Tomo I). Comité Nacional Español de Grandes Presas y Colegio de Ingenieros de Caminos, Canales y Puertos, España, 2003.
- Guía Técnica de Seguridad de Presas Nº 6. Construcción de presas y control de calidad. Comité Nacional Español de Grandes Presas y Colegio de Ingenieros de Caminos, Canales y Puertos, España, 1999.
- Manual de túneles y obras subterráneas. E.T.S.I. Minas, UPM, España, 2000.
- Analysis of Concrete and Masonry Dam Incidents. UNICIV Report 373, University of New South Wales, Australia, 1998.
- Open Pit Blast Design. Julius Kruttschnitt Mineral Research Centre, The University of Queensland, Australia, 1996.
- Guidelines for the Assessment of Rock Foundations of Existing Concrete Gravity Dams, BC Hydro Report No. MEP67, Vancouver, British Columbia, Canada, 1995.
- Manual del vigilante de la presa. Ministerio de Obras Públicas, Dirección General de Obras Públicas, España, 1969.

4.8 Ciberseguridad/riesgos ciberfísicos.

4.8.1 Introducción.

Una presa es una infraestructura que depende para su correcta operación y explotación de toda una serie de equipamiento industrial y electromecánico. Estos equipos están integrados para su accionamiento en sistemas de control y supervisión que incluyen instrumentación, actuadores, controladores automáticos (PLC) unidades remotas, terminales de supervisión (HMI), etc. Además, existe toda una serie de sistemas que permiten monitorizar el estado de la presa (sistemas de auscultación), medida y registro de parámetros hidrológicos (aforos de caudal, niveles, etc.). Estos sistemas están integrados con cada vez mayor frecuencia en redes de comunicación, locales y remotas, convirtiendo una presa en un sistema ciberfísico, lo que hace que estas infraestructuras estén expuestas a una serie de amenazas que hasta muy recientemente no se habían considerado. Por otra parte, la forma en que se explotan las infraestructuras (mantenimiento, ingeniería, coordinación entre distintos actores, etc.) también introduce riesgos que deben ser gestionados.

En la actualidad nos encontramos en un escenario de riesgo sistémico, en el que un incidente de seguridad en el ámbito físico puede tener implicaciones para la ciberseguridad y viceversa, lo que hace necesaria una aproximación integral para la protección de estas infraestructuras.

En paralelo a cuestiones de carácter técnico, también existe legislación que implica, en algunos casos, la necesidad por parte de los titulares de las infraestructuras de adoptar una serie de medidas de protección, como son la LPIC y el reglamento que la desarrolla. De conformidad con lo ya comentado, estas medidas de seguridad deben seguir una aproximación de seguridad integral, lo que incluye la ciberseguridad. En aquellos casos en que una infraestructura haya sido incluida en el catálogo nacional de infraestructuras críticas (o que implica que su titular se convierte, a su vez, en un operador de II.CC.), el Plan de Seguridad de Operado (PSO) y los Planes de Protección Específicos (PPE) son la herramienta básica de gestión de la seguridad. También debe tenerse en cuenta en cada infraestructura, de resultar de aplicación en lo relacionado con los operadores de servicios esenciales, lo dispuesto en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y su desarrollo reglamentario contenido en el Real Decreto 43/2021, de 26 de enero.

Cabe decir que las infraestructuras industriales, específicamente sus sistemas de control y supervisión (tecnologías de la operación u OT), poseen características propias diferenciales de los sistemas de información corporativa (o tecnologías IT). Por esta razón, debe evitarse la traslación directa de prácticas de seguridad en sistema IT, que puede resultar inefectiva o en el peor caso afectar a la operación de la propia presa que se intenta proteger. La participación de expertos en ciberseguridad industrial es clave en esta cuestión.

Es importante señalar que la introducción a posteriori, sobre infraestructuras existentes, de medidas de seguridad suele condicionar de forma importante su efectividad a la vez

que suponer un esfuerzo mayor. Por esta razón, y como criterio general, se debe incorporar la ciberseguridad como parte integrante del proceso proyecto-construcción-explotación.

4.8.2 Debilidades habituales.

La guía CCN-CERT IA-04-16[2] publicada por el Centro Criptológico Nacional recoge un listado de debilidades habituales en organizaciones que gestionan infraestructuras que dependen para su operación de sistemas ciberfísicos. Todas ellas son de aplicación en grandes presas, y deben ser, por tanto, objeto de análisis por los responsables de estas infraestructuras al definir la estrategia de seguridad:

- Uso inadecuado de dispositivos portátiles.
- Trabajo de terceros.
- Inadecuada gestión de las interconexiones con otras redes.
- Gestión deficiente de copias de seguridad.
- Falta de concienciación del personal.
- Inadecuada gestión de cambios.
- Inexistencia de planes adecuados de gestión de incidentes y continuidad.
- Gestión deficiente de la información.
- Gestión deficiente del software.
- Asignación deficiente de responsabilidades y gestión de la seguridad.
- Gestión deficiente de usuarios y contraseñas.
- Falta de gestión técnica de la seguridad y sistemas.

Ilustración 16. Informe de Amenazas de CCN_CERT IA-04/16.

Estas debilidades suponen factores de riesgo que pueden contribuir a aumentar la probabilidad de que se materialice una amenaza u incrementar su impacto, y la organización debe disponer de controles técnicos, organizativos y procedimentales

[2] CCN-CERT, T. (2018). Risk Analysis in Industrial Control Systems (ICS). Report IA-04/16, Centro Criptologico Nacional, Madrid, 28 January 2016 (in Spanish).

destinados a la eliminación o minimización de las mismas. Estos aspectos se tratan con detalle en los siguientes puntos.

4.8.3 Activos.

La operación de una presa se apoya en un conjunto de activos formados por estructuras y elementos de obra civil, equipos electromecánicos e instrumentación, sistemas de control, supervisión y redes de comunicación. A ellos cabe añadir otros activos como el personal encargado de su operación y mantenimiento, propio o de terceros y la información sobre la misma generada durante el proceso proyecto-construcción-explotación. A continuación, se propone un listado de activos que deberían ser considerados desde el punto de vista de la ciberseguridad:

- Información accesible sobre los propios sistemas (casos de éxito de proveedores, documentación asociada al proceso proyecto/construcción/explotación, estudios académicos, web de organismos públicos o privados, etc.)
- Personal propio o de terceros encargado de la operación y mantenimiento.
- Interconexiones remotas para supervisión/mantenimiento.
- Interconexiones de integración en sistemas de gestión (redes SAIH…)
- Instrumentación y actuadores (sondas de nivel, caudalímetros, cámaras CCTV, detectores de intrusión, accionamientos de motores, válvulas o bombas, etc.
- Sistemas automatizados de propósito específico (auscultación, sistemas automáticos de alarma, etc.)
- Electrónica de red y comunicaciones (switches, routers, modem radio/3G/4G, pasarelas serie/Ethernet)
- Componentes de automatización (PLC, remotas, HMI locales).
- Sistemas de supervisión remotos o locales (servidores de tiempo real, estaciones de ingeniería, estaciones de operación, servidores de tiempos, etc.)
- Equipos auxiliares con opciones de gestión remota (SAI, grupos electrógenos de emergencia…)
- Sistemas de seguridad (monitorización, detección, alarma…)

4.8.4 Modos de fallo.

De conformidad con lo expuesto en puntos anteriores, los sistemas ciberfísicos son parte integrante de una presa moderna y pueden ser utilizados para alterar su correcta operación sin necesidad de recurrir a métodos físicos tradicionales como los tratados en otros puntos (ver, por ejemplo, el punto 4.6 sobre voladura o deterioro grave de elementos de una presa). Complementariamente, las amenazas de ciberseguridad pueden encontrase detrás de forma total o parcial de escenarios de riesgo ya analizados como el accionamiento malintencionado de compuertas, el sabotaje, etc.

El funcionamiento de una presa puede alterarse tanto de forma activa (por ejemplo, accionando las compuertas de forma directa) como pasiva (impidiendo que sean

accionadas cuando sea necesario) o incluso provocando una operación indebida por acción u omisión por parte de los responsables de la infraestructura por medio del falseo de la información recibida en los puestos de supervisión remota.

Siguiendo la clasificación recogida en el documento *The Industrial Control System Cyber Kill Chain* publicada por SANS-ICS[3] las acciones de un atacante se pueden clasificar de la siguiente manera:

- Pérdida de vision (Loss of view).
- Pérdida de control (Loss of control).
- Denegación de vision (Denial of view).
- Denegación de control (Denial of control).
- Denegación de seguridad (Denial of safety).
- Manipulación de visión (Manipulation of View).
- Manipulación de control (Manipulation of Control).
- Manipulación de sensores e instrumentos (Manipulation of Sensors and Instruments).
- Manipulación de seguridad (Manipulation of Safety).

Para interpretar las situaciones descritas anteriormente, debe tenerse en cuenta lo siguiente:

- *Denial* o denegación es la condición en la que se niega al operador del sistema el acceso o la capacidad de realizar una acción de forma temporal. Esto no tiene por qué resultar inmediatamente en un impacto sobre la operación de la infraestructura, ya que esto depende del tiempo en que se mantenga esta condición, del contexto en que se produzca, etc.
- *Loss* o pérdida es la condición en la cual se pierde la capacidad de supervisar el estado de un sistema (view) o el control efectivo del mismo (control). A diferencia de la denegación (*denial*) permanecerá incluso una vez se ha eliminado la interferencia del atacante.
- *Manipulation* o manipulación es la condición por la cual un atacante realiza acciones directamente contra un sistema con el fin de alterar su modo de funcionamiento, lo que resulta de forma inmediata en una modificación en las condiciones de operación de la infraestructura.

La aplicación de cada uno de ellos a un activo define los modos de fallo. Cabe considerar que el mismo resultado puede producirse por una acción deliberada o por una acción casual (un malware no dirigido o un error accidental en la operación).

[3] Assante, M. J., & Lee, R. M. (2015). The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, *1*.

Desde un punto de vista específico de ciberseguridad, y con un enfoque dirigido a los sistemas ciberfísicos, las amenazas consideradas son las siguientes:

- Interferencia en el software de supervisión.
- Interferencia en la electrónica de red y comunicaciones.
- Interferencia en las comunicaciones.
- Interferencia en el nivel de control.
- Interferencia en la instrumentación.
- Interferencia en los actuadores.

A continuación, se ofrece un conjunto de tablas que relacionan las amenazas existentes sobre los sistemas ciberfísicos de una presa, su aplicación a los activos establecidos anteriormente y algunos ejemplos del posible impacto asociado.

AMENAZA	SISTEMA AFECTADO	MECANISMO	OBJETIVO (SANS ICS)	POSIBLE IMPACTO	EJEMPLO
Interferencia software de supervisión	Sistema SCADA local o centralizado	Cifrado (ramsonware) de servidores de tiempo real, HMI.	Loss of view Denial of control	Imposibilidad de visualizar el estado del sistema remoto o de actuar sobre el mismo.	Imposibilidad de visualizar el estado actual (niveles, aforos, posición de compuertas) o actuar a través de las interfaces HMI del sistema.
	Sistema SCADA local o centralizado	Acceso no autorizado a interfaces de supervisión o gestión.	Loss of safety Denial of view Denial of control	Realización de operaciones indebidas.	Apertura o cierre de compuertas. Eliminación de usuarios legítimos. Cambios de configuración, despliegues, etc.
	Sistema SCADA local o centralizado	Acceso no autorizado al software.	Denial of view Loss of view Denial of control Loss of control Manipulation of view	Realización de operaciones indebidas. Funcionamiento del sistema impredecible. Falseo de la información recibida por los operadores.	Uso del sistema para acceder a otras infraestructuras remotas.

Tabla 6. Amenazas existentes sobre los sistemas ciberfísicos de una presa. Interferencia software de supervisión

AMENAZA	SISTEMA AFECTADO	MECANISMO	OBJETIVO (SANS ICS)	POSIBLE IMPACTO	EJEMPLO
Interferencia en electrónica de red y comunicaciones	Switches, pasarelas serie/Ethernet, routers, modem (3G/4G/radio) etc.	Modificación de la configuración de red.	Denial of view Loss of view Denial of control Loss of control	Imposibilidad de visualizar el estado del sistema remoto o de actuar sobre el mismo. Funcionamiento del sistema impredecible debido a la pérdida de comunicaciones entre sus componentes (instrumentación, actuadores, controladores, estaciones remotas, etc.)	Imposibilidad de visualizar el estado actual (niveles, aforos, posición de compuertas) o actuar a través de las interfaces HMI del sistema o, incluso, en modo local.
Interferencia en las comunicaciones	Redes de comunicación	MitM	Manipulation of view Loss of safety	Falseo de la información recibida por los operadores. Realización de operaciones indebidas por parte de los operadores.	Representación de valores falsos (cotas de lámina de agua, posición de compuertas…)

Tabla 7. Amenazas existentes sobre los sistemas ciberfísicos de una presa. Interferencias en electrónica de red y comunicaciones.

AMENAZA	SISTEMA AFECTADO	MECANISMO	OBJETIVO (SANS ICS)	POSIBLE IMPACTO	EJEMPLO
Interferencia en nivel de control	PLC, remotas, etc.	Escritura de registros en la memoria del PLC/remota	Loss of control Loss of safety Manipulation of view	Realización de operaciones indebidas. Funcionamiento del sistema impredecible.	Apertura o cierre de compuertas.

			Manipulation of control	Falseo de la información recibida por los operadores. Activación/inhibición de alarmas.	
	PLC, remotas, etc.	Comando de parada	Loss of control Loss of safety Loss of view	Funcionamiento del sistema impredecible.	Parada del PLC que detiene la regulación automática y la capacidad de actuación/visualización remota de ciertas variables.
	PLC, remotas, etc.	Manipulación de la configuración, programa, etc.	Loss of control Loss of safety Loss of view Manipulation of control	Funcionamiento del sistema impredecible. Realización de operaciones indebidas.	Modificación del programa en un PLC para que funciones de forma no prevista.

Tabla 8. Amenazas existentes sobre los sistemas ciberfísicos de una presa. Interferencias en nivel de control.

AMENAZA	SISTEMA AFECTADO	MECANISMO	OBJETIVO (SANS ICS)	POSIBLE IMPACTO	EJEMPLO
Interferencia en instrumentación	Sensores, sondas, cámaras IP, instrumentación en general	Modificación de la configuración/calibración	Loss of control Loss of safety Loss of view Manipulation of sensors and instruments	Funcionamiento del sistema impredecible. Realización de operaciones indebidas por parte de los operadores. Falseo de la información recibida por los operadores. Activación/inhibición de alarmas. Pérdida de supervisión por imagen.	Realización de medidas incorrectas que mueven a los operadores a llevar a cabo acciones inadecuadas.

Tabla 9. Amenazas existentes sobre los sistemas ciberfísicos de una presa. Interferencias en instrumentación.

AMENAZA	SISTEMA AFECTADO	MECANISMO	OBJETIVO (SANS ICS)	POSIBLE IMPACTO	EJEMPLO
Interferencia en actuadores	Arrancadores, variadores de frecuencia, bombas, SAI, actuadores de válvulas motorizadas o neumáticas otro tipo de equipamiento.	Modificación de la configuración	Loss of control Loss of safety Loss of view Denial of control	Funcionamiento del sistema impredecible. Imposibilidad de actuar sobre el sistema remoto.	Modificación de la configuración de las opciones de comunicación de un arrancador estático, lo que puede impedir el accionamiento de un motor o bomba.
	Arrancadores, variadores de frecuencia, actuadores de válvulas motorizadas o neumáticas, SAI, grupos electrógenos, otro tipo de equipamiento.	Escritura de registros en la memoria del dispositivo	Loss of safety	Realización de operaciones indebidas.	Parada de un SAI dejando sin suministro eléctrico los equipos alimentados a partir del mismo.

Tabla 10. Amenazas existentes sobre los sistemas ciberfísicos de una presa. Interferencias en actuadores

4.8.5 Referencias.

- Assante, M. J., & Lee, R. M. (2015). The industrial control system cyber kill chain. SANS Institute InfoSec Reading Room, 1.
- CCN-CERT, T. (2018). Risk Analysis in Industrial Control Systems (ICS). Report IA-04/16, Centro Criptologico Nacional, Madrid, 28 January 2016 (in Spanish).
- Directiva 2022/2555 del Parlamento Europeo y del Consejo, conocida como **NIS2**, es la legislación en materia de ciberseguridad adoptada para toda la Unión Europea

4.9 Contaminación intencionada del agua embalsada.

4.9.1 Introducción

Cualquier sabotaje persigue condicionar violentamente la opinión de un tercero para lograr unos objetivos. De forma que la finalidad de un acto de sabotaje puede no ser sólo causar víctimas o daños económicos y medioambientales, sino desprestigiar a la organización o demostrar a la sociedad lo vulnerable que puede llegar a ser.

En el campo de la contaminación del agua se aplican las mismas reglas, no solamente se trataría de introducir sustancias en el agua que pudieran causar graves daños a las personas, sino de obligar a incumplir alguno de los parámetros que nos hemos impuesto como sociedad para preservar a largo plazo nuestra salud y el medio ambiente. A veces incluso pudiera ser suficiente con añadir trazadores o colorantes inocuos para causar alarma y preocupación, o hacer circular en los medios de comunicación o redes sociales, rumores y mentiras para desinformar y desacreditar a las instituciones o empresas que realizan la gestión.

4.9.2 Modos de fallo

El modo de fallo es la contaminación del agua en las diferentes fases de su almacenamiento o distribución, con la intención de causar un daño o descrédito sanitario, económico, institucional, medioambiental, generar alarma social, crear notoriedad informativa, etc.

El almacenamiento y la distribución del suministro de agua tiene varias fases (en alta y baja) con diferente comportamiento.

Existen numerosos casos de atentados relacionados con infraestructuras del agua y que se han descrito en el apartado 3: “Casos Históricos”.

En España no existen, por fortuna, sabotajes importantes conocidos de contaminación del agua.

La amenaza de contaminación en el entorno de un embalse tiene una baja probabilidad de ocurrencia, solo consta el caso de Dinamarca (2006), y debido a los grandes volúmenes necesarios para su contaminación y los elevados tiempos de residencia, limita poderosamente los daños sobre la salud humana. Aunque sea improbable, es posible y debemos estar preparados para afrontarla.

4.9.3 Legislación considerada

Se han considerado dos normativas que establecen los criterios de calidad de obligado cumplimiento de las aguas destinadas al consumo humano y las destinadas a la calidad ambiental de las masas de agua.

De ambos, el más restrictivo es el destinado a la calidad ambiental de las aguas superficiales por ser más actual su publicación.

- Real Decreto 817/2015, de 11 de septiembre, por el que se establecen los criterios de seguimiento y evaluación del estado de las aguas superficiales y las normas de calidad ambiental
- Real Decreto 140/2003, de 7 de febrero, por el que se establecen los criterios sanitarios de la calidad del agua de consumo humano

4.9.4 Productos tóxicos potencialmente utilizados para contaminar el agua

Existe un gran número de compuestos que podrían ser desplegados por terroristas o personas malintencionadas en un ataque al suministro de agua y que internacionalmente se denominan agrupando sus iniciales, como Nucleares, Biológicos, Químicas y Radiológicas (NBQ-R):

- **Compuestos químicos usados en el tratamiento del agua:** Estos compuestos, como puede ser el cloro o el flúor, que mejoran la calidad del agua en las dosis adecuadas, pueden volverse tóxicos en cantidades excesivas. Estos químicos son muy fáciles de obtener, puesto que ya se encuentran dentro de las instalaciones, y un inadecuado manejo, intencionado o accidental, puede tener graves consecuencias. Además, en sistemas automatizados, pueden ser objeto de ciberataques y causar daños desde miles de kilómetros de distancia.
- **Metales pesados:** Los metales pesados son agentes peligrosos debido a su toxicidad para los seres humanos (mercurio, cadmio, plomo, níquel, etc.). También son bastante fáciles de obtener, y sus sales suelen ser fácilmente solubles.
- **Herbicidas:** Como una clase general, los herbicidas tienden a ser menos perjudiciales al ser humano que algunos otros compuestos, aunque hay algunas excepciones notables. Sin embargo, son muy fáciles de conseguir en grandes cantidades, de distribuir, y su presencia pasa desapercibida en el mundo rural, lo que aumenta su posible uso en embalses, balsas, canales, etc. Aunque no provocarían muchas muertes, el pánico causado por su presencia en redes de distribución podría ser grave.
- **Insecticidas:** Tienden a ser más perjudiciales para la salud del ser humano que los herbicidas. Algunos de los insecticidas tienen estructuras químicas muy similares a algunos de los agentes de guerra química. Como los herbicidas, los insecticidas también están disponibles en grandes cantidades y son fáciles de distribuir. En algunos casos, su solubilidad limita su utilidad como armas introducidos en el agua, pero otros son muy solubles y suponen una clara amenaza.
- **Nematocidas y rodenticidas:** Los nematocidas (plaguicidas de animales diminutos en forma de gusano) son similares a los insecticidas. Con algunas excepciones, tienden a ser más solubles que los insecticidas. Algunos compuestos nematocidas también son similares a agentes de guerra química en su estructura y modo de acción. Los rodenticidas (pesticidas que se utilizan para matar roedores) son motivo de preocupación ya que están diseñados

específicamente para ser letales para especies de mamíferos como los seres humanos. Ambas clases están disponibles en grandes cantidades.

- **Productos** químicos **industriales y diversos agentes:** Hay una infinidad de productos químicos industriales que podrían utilizarse en un ataque. El principal es el cianuro, ampliamente utilizado en minería y otras industrias.
- **Radionucleidos:** El uso de radionucleidos como arma es una clara posibilidad. Incluso si las víctimas son bajas, el impacto psicológico de una amenaza radiológica podría ser grave. Los compuestos de alta pureza, material altamente radiactivo, como el plutonio o uranio 238, son difíciles y caros de conseguir, y es poco probable que una organización terrorista que haya obtenido estos materiales esté dispuesta a utilizarlos en un ataque a un sistema de abastecimiento. Lo más probable es el uso de materiales radiactivos de nivel bajo o residuos.
- **Agentes de guerra:** agentes de guerra química como VX, Soman, Sarín o Gas Mostaza. No es probable que se utilizara contra el sistema de abastecimiento de agua porque sus efectos en vía aerosol son mucho más devastadores.
- **Toxinas y Bioagentes:** Hay un número de protozoos, bacterias, virus y toxinas que podrían utilizarse en un ataque. Muchos de estos materiales son extremadamente tóxicos, con compuestos tales como toxina botulínica, siendo algunas de las sustancias más tóxicas conocidas. Estos tipos de materiales son bastante fáciles de obtener, hay varios ejemplos de la producción de ricina por terroristas con estos fines (Inglaterra, 2010). Las bacterias también se pueden cultivar fácilmente, de hecho, incluso las aguas residuales podrían ser utilizadas como un contaminante potencial de un ataque de reflujo.

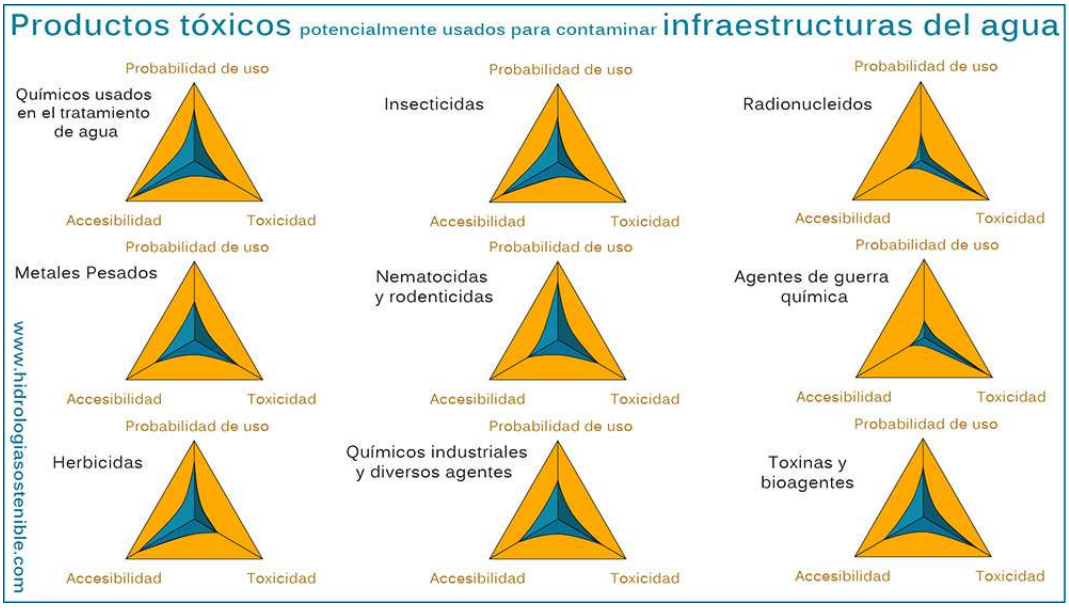

Ilustración 17. Productos tóxicos potencialmente utilizados para contaminar infraestructuras del agua.

4.9.5 Conclusiones de la contaminación intencionada del agua.

La probabilidad de ocurrencia de una contaminación malintencionada de sustancias tóxicas en un embalse es realmente baja, como lo atestiguan los escasos casos registrados (un único caso en Dinamarca, 2006). Más improbable es aún que esta contaminación del embalse produzca afección al ser humano, por cuanto que existe un gran volumen de dilución y un tiempo de respuesta muy importante. Sin embargo, es un riesgo posible y por lo tanto debemos estar preparados para afrontarlo.

5 ANÁLISIS DE RIESGOS.

La ley 8/2011, por la que se establecen medidas para la protección de las infraestructuras críticas, en su artículo 2, define "*análisis de riesgos*", como *el estudio de las hipótesis de amenazas posibles, necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo*.

5.1 Metodología a emplear

Con el objetivo de identificar y gestionar los principales riesgos a los que se encuentran expuestos los activos críticos de una infraestructura, es necesario utilizar una metodología o varias, contemplando la seguridad de una manera global, y analizando las amenazas, tanto físicas como lógicas existentes, que puedan afectar a cada uno de los activos.

Aunque existen muchas metodologías, tal vez, las más utilizadas a nivel internacional para el análisis de riesgos sean SEPTRI, MOSLER y MAGERIT.

La metodología SEPTRI evalúa las consecuencias en términos económicos y su ámbito de aplicación no se restringe a un peligro concreto, sino que es apto para evaluar cualquier factor de peligrosidad.

La metodología MOSLER es considerada como un método cuantitativo, aunque la clasificación del riesgo es considerada una fase cualitativa del mismo.

La metodología MAGERIT, está directamente relacionada con la generalización del uso de las tecnologías de la información, siendo esta elaborada por el Consejo Superior de Administración Electrónica.

Cabe destacar que la metodología SEPTRI y MOSLER son totalmente compatibles y complementarias por lo que se pueden utilizar de manera conjunta. Es habitual, por ejemplo, utilizar metodologías SEPTRI/MOSLER para la parte física y MAGERIT para la parte de ciberseguridad en sistemas corporativos o puramente IT, sin olvidar la necesidad de integración de las tres metodologías basadas en los términos de probabilidad e impacto como resultado del riesgo. Además, existen metodologías específicas para la realización de análisis de riesgos de equipamientos y sistemas industriales, como por ejemplo la descrita en la norma IEC 62443 (parte 3-2).

5.2 Índice de Vulnerabilidad.

Sea cualesquiera la metodología utilizada, lo primero que se debe plantear es la determinación de la Vulnerabilidad de cada uno de los activos de la infraestructura.

Para su determinación, en esta Guía se utiliza la documentación del proyecto BIA2010-17852 “Incorporación de los componentes de Riesgo Antrópico a los sistemas de gestión integral de Seguridad de presas y embalses”, desarrollado en el periodo 2011-2013 en la Universidad Politécnica de Valencia (UPV), financiado por el Ministerio de Ciencia e Innovación en el marco del Plan Nacional de I+D+i 2008-2012.

La tabla siguiente se resume los niveles de análisis de riesgo antrópico que se pueden plantear y sus características.

Nivel	Tipo	Objeto	Uso de modelos de riesgo	Probabilidad de fallo	Consecuencias	Vulnerabilidad del sistema	Resultados riesgo	Toma de decisiones
Básico (B)	Cualitativo Cuantitativo	Análisis preliminar	No	No	Básico a intermedio	Básico	No	Cribado (screening) Identificación de la necesidad de estudios de detalle.
Intermedio (I)	Cualitativo Cuantitativo	Análisis global del portfolio de presas	Amenazas naturales	Probabilidad de fallo por amenazas naturales (escenario hidrológico)	Intermedio	Básico a intermedio	Riesgo en escenario hidrológico Riesgo antrópico condicional	Gestión del sistema Análisis de medidas de reducción del riesgo
Avanzado (A)	Cuantitativo	Análisis detallado a nivel global (portfolio) e individual (presa)	Amenazas naturales y amenazas antrópicas	Sí	Intermedio a avanzado	Intermedio a avanzado	Sí	Gestión integral del sistema Optimización y priorización de medidas de reducción del riesgo

Tabla 11. Niveles de análisis del riesgo antrópico en presas. Fuente: Proyecto BIA2010-17852.

Para el **nivel básico**, se propone un índice global de consecuencias para escenarios de ataque identificados para el sistema, que se expone en la tabla siguiente:

Descriptor Categoría	Muy alto Puntuación = 10	Alto Puntuación = 8	Medio Puntuación = 6	Bajo Puntuación = 4	Muy bajo Puntuación = 2
Sociedad	Población en riesgo (PAR): PAR > 1.000	Población en riesgo: (PAR = 100-1.000)	Población en riesgo: (PAR = 10-100)	Población en riesgo: (PAR = 1 - 10)	No existe población en riesgo
Economía	Interrupción de servicios esenciales a escala nacional o pluriregional (>1.000 M€)	Interrupción de servicios esenciales a escala pluriregional (100 - 1.000 M€)	Interrupción de servicios esenciales a escala regional (10 - 100 M€)	Interrupción de servicios esenciales a escala local o regional (< 10 M€)	No hay interrupción de servicios esenciales Daños locales
Medio ambiente	Daño medioambiental muy grave o irreparable	Daño medioambiental grave o de difícil recuperación	Daño medioambiental grave a moderado y de 1 a 2 años de recuperación	Daño medioambiental moderado (<1 año de recuperación)	Daño medioambiental leve

Tabla 12. Ejemplo de estimación de consecuencias a nivel cualitatitvo (DAMSE, 2008).

Además, se incluye un índice global de vulnerabilidad como análisis preliminar en sistemas presa-embalse para riesgo antrópico que depende de los siguientes factores:

- ACCESIBILIDAD
    - Accesibilidad a coronación y cuerpo de presa: por carretera, camino secundario, camino privado, barreras.

  - Accesibilidad al aliviadero / Órgano de Desagüe (OD): desde carretera sin barreras hasta perímetro cerrado.

- CONTROL ALIVIADEROS/ÓRGANOS DE DESAGÜE
  - Accesibilidad a mandos de control: barreras, zona accesible.
  - Accionamiento de mandos: activado, posible activación o desconectado.
- SEGURIDAD y DETECCIÓN
  - Sistemas de seguridad: cámaras, sensores y alarmas
  - Personal de la presa: Presencia permanente/habitual/ocasional de personal en la presa.
  - Inspección frecuente/diaria, semanal u ocasional.
- COMUNICACIÓN:
  - Varias vías de comunicación, suministro independiente, fallos, cobertura.
- RESPUESTA:
  - Fuerzas de seguridad: vigilancia y visitas por parte de fuerzas de seguridad, acceso, frecuencia y comunicación con el personal.

Estos factores, agrupados en cinco categorías, se analizan a partir de la información existente en la documentación de cada presa y, fundamentalmente, a partir de la recogida de datos efectuada durante visitas de campo. Cada uno de los factores descritos anteriormente se evalúa empleando los descriptores de la Tabla 17 y asignando los pesos definidos en la Tabla 16.

Categoría	Subcategoría	Peso (w)
ACCESIBILIDAD	Presa	10
	Aliviaderos y órganos de desagüe	15
CONTROL OD	Acceso controles	10
	Activación controles	5
SEGURIDAD/ DETECCIÓN	General	20
	Personal de la presa	10
	Detección incidente	10
COMUNICACIÓN	Comunicación interior/exterior	10
RESPUESTA	Fuerzas de seguridad	10
Total		100

Tabla 13. Pesos establecidos para las categorías de cálculo del índice global de vulnerabilidad. Fuente: Proyecto BIA2010-17852.

Por tanto, el índice global de vulnerabilidad se obtiene de la siguiente expresión:

$$IGV = \frac{\sum_{i=1}^{n} w_i d_i}{\sum_{i=1}^{n} w_i}$$

donde *i* indica la subcategoría considerada (de un total de n=9 subcategorías), w_i es el peso de cada subcategoría y d_i es el valor numérico correspondiente al descriptor asignado.

Un índice bajo indica una presa con baja accesibilidad, mayor posibilidad de detección de incidentes, mejores comunicaciones, un elevado nivel de vigilancia, etc. El valor máximo del índice global de vulnerabilidad es igual a 5.

Este índice caracteriza la vulnerabilidad general de la presa frente a amenazas antrópicas (no considera la vulnerabilidad de cada elemento por separado, ni las consecuencias potenciales).

A continuación, se muestra una tabla con indicaciones para la asignación de valores para cada subcategoría en función de las características de la presa.

Categoría	Subcategoría	Valores propuestos del descriptor de vulnerabilidad del sistema (d)
ACCESIBILIDAD	ACCESIBILIDAD (I) Accesibilidad a coronación y cuerpo de presa	5: por carretera 1: camino privado/barreras
	ACCESIBILIDAD (II) Accesibilidad al aliviadero / OD	5: desde carretera, sin barreras 1: perímetro cerrado
CONTROL OD	ACCESIBILIDAD (III) Accesibilidad a mandos de control	1: varias barreras 5 : zona accesible, sin barreras
	ACCIONAMIENTO MANDOS	5: corriente 3: desconectado, pero activación posible 1:desconectado
SEGURIDAD/ DETECCIÓN	SISTEMAS DE SEGURIDAD	5: No existen sistemas de seguridad/vigilancia 3: Cámaras 2: Cámaras y alarmas 1: Cámaras, sensores de movimiento.
	DETECCIÓN INCIDENTE	5: Inspección inusual 3: Semanal 1: Inspección diaria
	PRESENCIA DE PERSONAL Presencia de personal en la presa	5: localización remota 2: a diario, pero no hay poblado 1: personal reside en las proximidades de la presa
COMUNICACIÓN	COMUNICACIÓN Sistemas de comunicación	5: fallos, sin cobertura 1: varias vías, funcionamiento independiente
RESPUESTA	FUERZAS DE SEGURIDAD Vigilancia Fuerzas de seguridad	5: Muy Bajo (no hay protocolos de comunicación, ni visitas) 3: Medio (visita inusual, pero llaves y acceso) 1: Muy Alto (visitas frecuentes, comunicación)

Tabla 14. Tabla de estimación de la vulnerabilidad del sistema a nivel cualitativo.

A partir de estos índices asignados a cada categoría, se obtiene un índice global que identifica la vulnerabilidad del sistema presa-embalse, tal y como recoge la tabla siguiente.

Descriptor (referente a vulnerabilidad del sistema)	Valor asignado (d)
Muy Alta	5
Alta	4
Media	3
Moderada	2
Baja	1

Tabla 15. Descriptores empleados para el cálculo del índice global de vulnerabilidad.

5.3 Análisis de cada Activo

A continuación, se realiza una descripción de los principales elementos del análisis de riesgos de una obra hidráulica de regulación. Cada amenaza requiere un análisis particular y los valores asignados en la tabla siguiente a los niveles de riesgo, son sólo recomendaciones generales (sólo para la versión completa):

ANÁLISIS DE RIESGO		
Activo	Dimensión	Amenaza
Agua Embalsada	Física	Envenenamiento Masivo
Cuerpo de presa + galerías	Física	Explosivos en personas suicidas
		Explosivos en vehículos terrestres tripulados (suicidas)
		Explosivos en vehículos terrestres no tripulados
		Explosivos en aeronaves no tripuladas
		Explosivos en lanchas o botes tripulados
		Explosivos en lanchas o botes no tripulados
		Explosivos en vehículos parados
		Explosivos colocados o abandonados
		Ataques con lanzagranadas/morteros
		Ataque terrorista armado
		Incendio intencionado
		Amenaza de Bomba
		Robo
		Vandalismo
		Ocupación Indebida
		Hurto
Pantalla de impermeabilización	Física	Explosivos en aeronaves no tripuladas
		Explosivos colocados o abandonados

		Ataques con lanzagranadas/morteros
		Ataque terrorista armado
		Vandalismo
Sistema de Drenaje en Galerías	Física	Explosivos en personas suicidas
		Explosivos colocados o abandonados
		Ataque terrorista armado
		Ocupación Indebida
Aliviaderos	Física	Explosivos en personas suicidas
		Explosivos en vehículos terrestres no tripulados
		Explosivos en lanchas o botes tripulados
		Explosivos en vehículos parados
		Ataques con lanzagranadas/morteros
		Ataque terrorista armado
		Incendio intencionado
		Amenaza de Bomba
		Robo
		Vandalismo
		Ocupación Indebida
		Sabotaje
		Hurto
Desagüe de fondo	Física	Explosivos en personas suicidas
		Explosivos en vehículos terrestres tripulados (suicidas)
		Explosivos en vehículos terrestres no tripulados
		Explosivos en aeronaves no tripuladas
		Explosivos en vehículos parados
		Explosivos colocados o abandonados
		Ataques con lanzagranadas/morteros

		Ataque terrorista armado
		Incendio intencionado
		Amenaza de Bomba
		Robo
		Vandalismo
		Ocupación Indebida
		Sabotaje
		Hurto
Toma	Física	Explosivos en personas suicidas
		Explosivos en vehículos terrestres tripulados (suicidas)
		Explosivos en vehículos terrestres no tripulados
		Explosivos en aeronaves no tripuladas
		Explosivos en vehículos parados
		Explosivos colocados o abandonados
		Ataques con lanzagranadas/morteros
		Ataque terrorista armado
		Incendio intencionado
		Amenaza de Bomba
		Robo
		Vandalismo
		Ocupación Indebida
		Sabotaje
		Hurto
Edificio Sala de Emergencia / Archivo Técnico	Física	Explosivos en personas suicidas
		Explosivos en vehículos terrestres tripulados (suicidas)
		Explosivos en vehículos terrestres no tripulados
		Explosivos en aeronaves no tripuladas
		Explosivos en vehículos parados

		Explosivos en paquetes enviados por correo
		Explosivos colocados o abandonados
		Ataques con lanzagranadas / morteros
		Ataque terrorista armado
		Incendio intencionado
		Amenaza de Bomba
		Robo
		Vandalismo
		Ocupación Indebida
		Sabotaje
		Hurto
Edificio Administrativo o de control	Física	Explosivos en personas suicidas
		Explosivos en vehículos terrestres tripulados (suicidas)
		Explosivos en vehículos terrestres no tripulados
		Explosivos en aeronaves no tripuladas
		Explosivos en vehículos parados
		Explosivos en paquetes enviados por correo
		Explosivos colocados o abandonados
		Ataques con lanzagranadas/morteros
		Ataque terrorista armado
		Incendio intencionado
		Amenaza de Bomba
		Robo
		Vandalismo
		Ocupación Indebida
		Sabotaje
		Hurto
Personal de la presa	Confidencialidad	Agresión y extorsión

		Ingeniería Social
	Física	Agresión y extorsión
		Ingeniería Social
	Disponibilidad	Agresión y extorsión
		Ingeniería Social

Tabla 16. Principales elementos del análisis de riesgos de una obra hidráulica de regulación.

En las siguientes tablas se recogen las potenciales amenazas identificadas más significativas:

Código Riesgo: RF.01	Amenaza: Envenenamiento Masivo
Descripción: Un actor u organización maliciosa, realiza vertidos en el agua embalsada con el fin de contaminar o envenenar el agua de manera que no pueda ser utilizada para el consumo o/y el regadío.	

Código Riesgo: RF.02	Amenaza: Daños producidos por explosivos transportados por personas
Descripción: Un actor u organización malicioso, ataca con explosivos elementos físicos de la presa con el fin de conseguir su inutilización o provocar accidentes graves aguas abajo con repercusión en la población afectada.	

Código Riesgo: RF.03	Amenaza: Daños producidos por terrorista armado
Descripción: Un actor u organización malicioso, ataca con explosivos elementos físicos de la presa con el fin de conseguir su inutilización o provocar accidentes graves aguas abajo con repercusión en la población afectada.	

Código Riesgo: RF.04	Amenaza: Daños producidos por amenaza de bomba
Descripción: Un actor u organización malicioso, ataca con explosivos elementos físicos de la presa con el fin de conseguir su inutilización o provocar accidentes graves aguas abajo con repercusión en la población afectada.	

Código Riesgo: RF.05	Amenaza: Daños producidos por explosivos en vehículos terrestres

Descripción: Un actor u organización malicioso, ataca con explosivos elementos físicos de la presa con el fin de conseguir su inutilización o provocar accidentes graves aguas abajo con repercusión en la población afectada.

Código Riesgo: RF.06	Amenaza: Daños producidos por explosivos en lanchas o botes
Descripción: Un actor u organización malicioso, ataca con explosivos elementos físicos de la presa con el fin de conseguir su inutilización o provocar accidentes graves aguas abajo con repercusión en la población afectada.	

Código Riesgo: RF.07	Amenaza: Daños producidos por explosivos en aeronaves
Descripción: Un actor u organización malicioso, ataca con explosivos elementos físicos de la presa con el fin de conseguir su inutilización o provocar accidentes graves aguas abajo con repercusión en la población afectada.	

Código Riesgo: RF.08	Amenaza: Agresión y extorsión
Descripción: Un actor u organización malicioso actúa sobre un empleado de la compañía con el fin de cometa o colabore en la comisión de actos delictivos que afecten al servicio esencial que la presa proporciona a la población. La actuación sobre el empleado puede ser agresiva, coaccionadora o psicológica.	

Código Riesgo: RF.09	Amenaza: Indisponibilidad provocada del personal
Descripción: Un actor u organización malicioso actúa sobre un empleado de la compañía con el fin de cometa o colabore en la comisión de actos delictivos que afecten al servicio esencial que la presa proporciona a la población. La actuación sobre el empleado puede ser agresiva, coaccionadora o psicológica.	

Código Riesgo: RF.10	Amenaza: Ingeniería social
Descripción: Un actor u organización malicioso actúa sobre un empleado de la compañía con el fin de cometa o colabore en la comisión de actos delictivos que afecten al servicio esencial que la presa proporciona a la población. La actuación sobre el empleado puede ser agresiva, coaccionadora o psicológica.	

Código Riesgo: RF.11	Amenaza: Delincuencia común

Descripción: Un actor u organización maliciosa (no de carácter terrorista) accede ilegalmente a dependencias de la presa para realizar hurtos o robos con fines principalmente lucrativos.

Código Riesgo: RF.12	Amenaza: Ocupación indebida
Descripción: Un actor u organización maliciosa (no de carácter terrorista) accede ilegalmente a dependencias de la presa con el objetivo de ocupar alguna instalación impidiendo su correcta gestión.	

Código Riesgo: RF.13	Amenaza: Daños causados por público en general
Descripción: Acciones producidas por vandalismo	

Código Riesgo: RF.14	Amenaza: Daños causados por Sabotaje
Descripción: Acciones producidas por delincuentes o público en general sin fines lucrativos que pueden afectar el normal funcionamiento de la presa	

Código Riesgo: RF.15	Amenaza: Daños causados por incendio intencionado
Descripción: Acciones producidas por delincuentes o público en general sin fines lucrativos que pueden afectar el normal funcionamiento de la presa	

Código Riesgo: RT.01	Amenaza: Acceso a Documentación técnica de la presa
Descripción: Acceso no autorizado a documentación técnica de la presa disponible en sistemas informáticos locales o remotos. Esto podría facilitar un ataque por parte de un delincuente.	

Código Riesgo: RT.02	Amenaza: Interferencia en el software de supervisión.
Descripción: Acciones realizadas sobre el software de supervisión (interfaces SCADA, HMI, etc.) que impidan la realización de operaciones remotas o locales, el reconocimiento del estado actual del sistema o que muestren un estado ficticio que provoque la realización de maniobras indebidas.	

Código Riesgo: RT.03	Amenaza: Interferencia en la electrónica de red y comunicaciones.
Descripción: Acciones realizadas sobre la configuración o disponibilidad de equipos de comunicaciones (routers, firewalls, switches, pasarelas…) que impidan el correcto funcionamiento del sistema, bien impidiendo el normal funcionamiento de las redes de comunicación o impidiendo el acceso remoto a estos dispositivos.	

Código Riesgo: RT.04	Amenaza: Interferencia en las comunicaciones.
Descripción: Acciones realizadas sobre las comunicaciones, por ejemplo intercepción o modificación de la información trasmitida.	

Código Riesgo: RT.05	Amenaza: Interferencia en el nivel de control.
Descripción: Acciones realizadas sobre equipamiento en el nivel de control (PLC, controladores, etc.) que resulten en un funcionamiento no previsto de los sistemas de regulación automática.	

Código Riesgo: RT.06	Amenaza: Interferencia en la instrumentación.
Descripción: Acciones realizadas sobre la instrumentación (caudalímetros, medidores de nivel, de presión, indicadores de posición, etc.) que afecten a su funcionamiento normal, provocando un funcionamiento imprevisto o la realización de maniobras indebidas (modificación en la calibración, por ejemplo).	

Código Riesgo: RT.07	Amenaza: Interferencia en actuadores.
Descripción: Acciones realizadas sobre los actuadores (apertura/cierre de compuertas, por ejemplo) que resulten en resultados no esperados o catastróficos.	

Tabla 17. Amenazas detectadas más significativas.

6 MEDIDAS DE SEGURIDAD.

Atendiendo a las Resoluciones del 15 y 29 de noviembre de 2011, de la Secretaría de Estado de Seguridad, sobre "*Contenidos mínimos del Plan de Protección Específico*", hay tres tipos de medidas:

6.1 Medidas Organizativas o de gestión

El Operador deberá indicar si dispone de al menos de las siguientes medidas organizativas o de gestión, y el alcance de cada una de ellas:

- Análisis de Riesgos: Evaluación y valoración de las amenazas, impactos y probabilidades para obtener un nivel de riesgo.
- Definición de roles y responsabilidades: Asignación de responsabilidades en materia de seguridad.
- Cuerpo normativo definido: políticas, procedimientos y estándares de seguridad
- Normas y/o regulaciones de aplicación a la infraestructura estratégica o crítica, así como identificación de su nivel de cumplimiento.
- Certificación, acreditación y evaluación de seguridad obtenidas para la infraestructura crítica o estratégica.
- Certificación de "espacio seguro" en situación de epidemia sanitaria.

6.2 Medidas Operacionales o procedimentales

- Procedimientos para la realización, gestión y mantenimiento de activos
- Procedimientos de Contingencia / Recuperación, en función de los escenarios de contingencia que hayan sido definidos
- Procedimientos de formación, concienciación y capacitación
- Procedimientos operativos para la monitorización, supervisión y evaluación/auditoría
- Procedimientos para la gestión de acceso
- Procedimiento para la realización de análisis de calidad de las aguas
- Procedimientos operacionales del personal de seguridad (funciones, horarios, dotaciones, etc.).
- Procedimientos de gestión y respuesta de incidentes
- Procedimientos de realización y prueba de copias de seguridad.
- Procedimiento para la gestión de usuarios y credenciales.
- Procedimientos de bastionado de equipos.
- Procedimientos de gestión de vulnerabilidades.
- Realización de evaluaciones periódicas de ciberseguridad en los sistemas industriales.
- Procedimientos para la gestión del trabajo de terceros.

6.3 Medidas de Protección o Técnicas.

6.3.1 Medidas de Prevención:

El contenido de este apartado es restringido.

6.3.2 Medidas de Detección:

El contenido de este apartado ha sido limitado.

- Riesgos físicos.
  - Detectores de intrusión, cámaras de video-vigilancia / CCTV
  - Medidas para el control de paquetes y detección de sustancias tóxicas, explosivos, etc.
  - Lectores de matrículas
  - Detector de temperatura y mascarilla en situación de pandemia sanitaria.
  - Detección precoz del incidente mediante el video-vigilancia y sensores de intrusión en los puntos de acceso.
  - Detectores de apertura y manipulación de cuadros de control.
  - Disponer de sistemas de avisos y alarmas a personas responsables ante movimientos en órganos de desagüe.
  - Intercomunicación con las Fuerzas y Cuerpos de Seguridad del Estado (FCS).

- Riesgos de ciberseguridad
  - Protección antimalware.
  - Despliegue de sistemas de monitorización (sistemas de detección de intrusos, tanto en red como en clientes NIDS/HIDS; sistemas de recolección de logs…)

6.3.3 Coordinación y Monitorización:

- Centro de Control de Seguridad (control de alarmas, recepción y visionado de imágenes, etc.).
- Centro de operaciones de seguridad lógica (también puede estar englobado en el anterior).
- Equipos de vigilancia (turnos, rondas, volumen, etc.).
- Sistemas de comunicación

7 PROPUESTA DE MEJORAS

El camino a recorrer para la protección de las infraestructuras hidráulicas estratégicas es arduo y no podemos completar su implantación en unos pocos años. Es lógico pensar

que la implementación de una nueva forma de actuar requerirá de algunas décadas para poderla llevar a cabo, especialmente si consideramos lo que estamos tardando en implantar los Planes de Emergencias de Presas y Balsas, cuya primera directriz básica de protección civil era del año 1995 y hoy seguimos trabajando.

La pandemia del COVID-19 ha puesto de manifiesto la debilidad de la sociedad frente a virus de afecciones nacionales o universales. Ha demostrado la gran vulnerabilidad que ocasiona una trasmisión aérea y ha convertido el agua en una herramienta higiénica imprescindible de luchar contra el virus. También hemos aprendido que los análisis de las aguas residuales se convierten en un precursor-detector del comienzo de la pandemia. Una vez más, se ha demostrado la importancia estratégica y crítica de este servicio esencial.

A continuación, se exponen algunas ideas del Sector del Agua en las que deberemos trabajar en los próximos años o décadas.

- Desinversión en el sector del agua.
  En la última década en España, se ha dejado de invertir en infraestructuras hidráulicas, tanto desde el sector privado, cómo el público. Esto está causando una pérdida constante y masiva de recursos humanos, un envejecimiento de las plantillas y una deficiente inversión económica para mantenimiento y operación, que lastra la gestión y sobre todo la seguridad de la infraestructura.
  Las causas están motivadas por la crisis económica y el endeudamiento público, un cambio de los criterios de inversión apostando por otras energías renovables, dejando abandonadas las hidráulicas y un menor control público debido a la escasez de funcionarios que puedan requerirlo. Cada vez los trabajadores del sector del agua, son menos, más genéricos, tienen menos experiencia, tienen menos controles públicos que les exijan tomar medidas, cuando las solicitan las inversiones no llegan y las tareas de su jornada son cada vez mayores.

  El sector privado mucho más ágil en la adaptación, ante este fenómeno de restricción de recursos humanos, ha impulsado una creciente automatización, y centralización de recursos. Esto es sin duda una ventaja en algunos aspectos, pero también tiene sus desventajas:
    - Problemas en caso de fallo para funcionar “en modo manual”.
    - Mayor dificultad de reacción rápida ante el fallo.
    - Necesidad de personal mucho más especializado, más difícil de formar y reemplazar.
    - Instalaciones sin presencia humana durante largos períodos de tiempo, mucho más fácil de sabotear.
    - En el campo de las presas, éxodo de profesionales de la ingeniería civil a otros sectores y predominio de la especialidad industrial, fomentando la producción sobre la seguridad.

- Medidas legislativas.

- Implementación de marcos legales de protección. Existe una desprotección frente al sabotaje informativo (desinformación, fake news, desprestigio) que, en un aspecto tan transcendental sanitariamente como el agua, puede crea una importante alarma social. El derecho a la información y libertad de prensa son reglas de convivencia que nos hemos impuesto en los países democráticos, pero tal vez se pudiera regular la trasmisión masiva de información no contrastada o fiable, la eliminación en redes sociales de fake news, o la inserción de un texto adicional señalándolo. Sin duda la emisión de datos oficiales homogéneos y contratados ayuda siempre a evitar malas interpretaciones, por lo que parece importante establecer protocolos estándares de emisión de datos oficiales.
- Marcos legales homogéneos. La normativa de presas no ha sido homogénea en el pasado, unas presas han estado sujetas al Reglamento y otras a la Instrucción, con criterios finales diferentes. La aprobación definitiva de las Normas Técnicas de Seguridad, por Real Decreto 264/2021 de 13 de abril, ha sido sin duda una gran ayuda, pero ahora queda su adaptación real.
- En algunas comunidades autónomas todavía no existe el órgano regulador de la seguridad de las presas y balsas fuera de cauce público.

- Integración de las medidas legislativas en las organizaciones.
  La mayoría de las empresas del sector del agua han incorporado en sus estructuras los nuevos procedimientos de gestión de la seguridad (Plan de seguridad del operador, Plan de protección específica, Plan de apoyo operativo y sus revisiones) y las nuevas figuras organizativas en sus plantillas (Responsable de seguridad y enlace, y Delegado de Seguridad). Sin embargo, la implantación real de estas nuevas normas legislativas está teniendo un menor grado de cumplimiento en la administración. Por un lado, las nuevas funciones, competencias y responsabilidad del Responsable de seguridad y enlace, y del Delegado de seguridad requieren de una modificación de la Relación de Puestos de Trabajo de la Administración, donde por ejemplo se debería reseñar la necesidad de contar con la habilitación de Director de Seguridad, tal y como establece la Ley 8/2011, de 18 de abril por el que se establecen medidas de protección de las infraestructuras críticas, y posiblemente incentivar su acceso con mejores complementos específicos. Por otro lado, los nuevos procedimientos de gestión requieren de inversión para poder implantarla.

- Complejidad e interdependencia con otros sectores estratégicos.
  El Subsector de Abastecimiento está muy atomizado. Esto puede ser una ventaja a efectos de criticidad porque no hay muchos usuarios afectados en caso de fallo. Sin embargo, también es una desventaja, porque es mucho más difícil prever una vulnerabilidad y más difícil de proteger

- Potenciar y fortalecer la relación de los titulares de presas con las Fuerzas y Cuerpos de Seguridad del Estado (F.C.S).
  Potenciar la gran disposición y profesionalidad de las F.C.S. que siempre han respondido a los requerimientos de los operadores, mediante la celebración de jornadas de formación, simulacros, visitas técnicas de las instalaciones, etc.

8 ANEXO I: CATALOGO DE AMENAZAS

Categoría	Código	Amenaza
Riesgos específicos de ciberseguridad	CYB.1	Interferencia en el software de supervisión: cifrado de servidores de tiempo real, acceso no autorizado a interfaces de supervisión o gestión…
	CYB.2	Interferencia en la electrónica de red y comunicaciones: modificación de la configuración de red, etc.
	CYB.3	Interferencia en las comunicaciones: ataques de Man-in-the-Middle, etc.
	CYB.4	Interferencia en el nivel de control: realización de operaciones indebidas, funcionamiento del sistema impredecible, falseo de la información recibida por los operadores, activación/inhibición de alarmas…
	CYB.5	Interferencia en la instrumentación: por ejemplo, modificación de la configuración/calibración de sensores.
	CYB.6	Interferencia en los actuadores: modificación de configuraciones, órdenes de marcha/paro de bombas, de apertura/cierre de compuertas, etc.
Accidentes, interdependencias y riesgos operacionales y técnicos	ACC.1	Accidente de transporte
	ACC.2	Fallo técnico
	ACC.3	Riesgos accidentales
Terrorismo y crimen organizado	TER.1	Explosivos en personas suicidas
	TER.2	Explosivos en vehículos terrestres tripulados
	TER.3	Explosivos en vehículos terrestres no tripulados
	TER.4	Explosivos en aeronaves no tripuladas
	TER.5	Explosivos en lanchas o botes no tripulados
	TER.6	Explosivos en lanchas o botes tripulados
	TER.7	Explosivos en vehículos parados

	TER.8	Explosivos en paquetes enviados por correo
	TER.9	Explosivos colocados o abandonados
	TER.10	Ataques con lanzagranadas/morteros
	TER.11	Ataque terrorista armado
	TER.12	Envenenamiento Masivo
	TER.13	Ataque químico
	TER.14	Ataque radiológico
	TER.15	Ataque nuclear
	TER.16	Incendio intencionado
	TER.17	Pulso electromagnético
Crímenes agresivos	CRA.1	Agresión y extorsión
	CRA.2	Sabotaje
	CRA.3	Amenaza de bomba
Delincuencia ordinaria	DEL.1	Robo
	DEL.2	Hurto
	DEL.3	Fraude
	DEL.4	Vandalismo
	DEL.5	Ocupación Indebida
Riesgos meteorológicos	MET.1	Inundaciones
	MET.2	Incendios
	MET.3	Tormenta
	MET.4	Tormenta eléctrica
	MET.5	Contaminación electromagnética
	MET.6	Marejada ciclónica
	MET.7	Huracanes
	MET.8	Tornados
	MET.9	Ola de calor
	MET.10	Ola de frío
	MET.11	Sequía
	MET.12	Nieve
	MET.13	Granizo
	MET.14	Hielo

Riesgos geofísicos	GEO.1	Terremotos
	GEO.2	Tsunamis
	GEO.3	Erupción volcánica
	GEO.4	Hundimientos
	GEO.5	Deslizamiento de tierras
	GEO.6	Tormenta Geomagnética
	GEO.7	Meteoritos
Amenazas de origen terrorista o malintencionado	ETM.1	Accionamiento malintencionado de compuertas
	ETM.2	Rotura de conductos
	ETM.3	Utilización de explosivos en compuertas
	ETM.4	Voladura o deterioro grave de elementos de la presa
	ETM.5	Obstrucción en conductos de aireación
	ETM.6	Manipulación del drenaje
	ETM.7	Contaminación intencionada del agua embalsada
	ETM.8	Contaminación intencionada del aire en galerías
Amenazas a la seguridad estructural o interna	ESI.1	Corte vías de acceso
	ESI.2	Avenidas
	ESI.3	Oleaje en el embalse
	ESI.4	Ciclos hielo-deshielo
	ESI.5	Cargas imprevistas sobre el dique
	ESI.6	Rotura de presas aguas arriba
	ESI.7	Caída de objetos de gran volumen en el embalse
	ESI.8	Sismo
	ESI.9	Corte persistente de la línea eléctrica
	ESI.10	Corte persistente de las comunicaciones
	ESI.11	Condiciones pluviométricas e hidrológicas según estacionalidad
Cuerpos de presas materiales sueltos	EMS.1	Degradación del rip-rap
	EMS.2	Mal función sistema de drenaje

	EMS.3	Obstrucción de drenes y filtros
	EMS.4	Biointrusión
	EMS.5	Acarcavamiento superficial
	EMS.6	Saturación temporal del espaldón de aguas abajo
	EMS.7	Apertura de cavidades o dolinas
	EMS.8	Sobretensiones en contactos entre estructuras rígidas y terraplenes
	EMS.9	Movimientos diferenciales
	EMS.10	Transferencia de carga
	EMS.11	Erosión interna (Sifonamiento)
	EMS.12	Licuefacción
	EMS.13	Sifonamiento
	EMS.14	Deslizamiento aguas arriba
	EMS.15	Deslizamiento aguas abajo
	EMS.16	Rotura en conductos en el interior de la presa
	EMS.17	Flujo anormal en conductos en el interior de la presa
	EMS.18	Rebosamiento
	EMS.19	Filtración de caudal importante
Cuerpos de presas de fábrica	EPF.1	Agrietamientos y fisuras
	EPF.2	Desalineaciones
	EPF.3	Movimientos diferenciales
	EPF.4	Deformaciones
	EPF.5	Degradación del material
	EPF.6	Sobretensiones
	EPF.7	Sobrevertido
	EPF.8	Obstrucción generalizada de drenes
	EPF.9	Deslizamiento de bloque
	EPF.10	Filtración de caudal importante en cuerpo de presa
	EPF.11	Corrosión
Cimientos	ERC.1	Movimientos de los cimientos

	ERC.2	Deformaciones y asientos
	ERC.3	Erosión interna (Tubicación)
	ERC.4	Degradación
	ERC.5	Hinchamiento
	ERC.6	Licuefacción
	ERC.7	Apertura de cavidades
	ERC.8	Dolinas
	ERC.9	Colapso de cavidades
	ERC.10	Helado de rellenos
	ERC.11	Socavaciones
	ERC.12	Sifonamiento
	ERC.13	Erosión del cimiento,
	ERC.14	Filtración de caudal importante en cimiento o estribos
Embalse	EMB.1	Saturación de las laderas del embalse
	EMB.2	Deslizamientos de laderas de grandes dimensiones
	EMB.3	Oleaje en el embalse producido por deslizamientos
	EMB.4	Nuevas vías de filtración en el vaso
	EMB.5	Formación vórtices en la superficie del agua o dolinas
	EMB.6	Colmatación del embalse
Instalaciones	EIN.1	Pérdida de control del dique
	EIN.2	Aislamiento del dique
	EIN.3	Manipulación incorrecta de válvulas
	EIN.4	Manipulación incorrecta de compuertas
	EIN.5	Destrucción de válvulas de los órganos de desagüe
	EIN.6	Deterioro de válvulas de los órganos de desagüe
	EIN.7	Destrucción de compuertas de los órganos de desagüe

	EIN.8	Deterioro de compuertas de los órganos de desagüe
Origen industrial	EOI.1	Emisiones electromagnéticas
	EOI.2	Avería
	EOI.3	Denegación del servicio por terceros
	EOI.4	Fallo del suministro eléctrico
Actividades contaminantes	EAC.1	Vertederos ilegales en la cuenca
	EAC.2	Vertidos ilegales a las masas de agua
Navegación	ENA.1	Daños sobre usos socioeconómicos derivados
	ENA.2	Daños sobre los frágiles ecosistemas acuáticos
Actividad humana indebida	EHI.1	Accesos no autorizados
	EHI.2	Controles no autorizados
	EHI.3	Divulgación de información sensible o clasificada
	EHI.4	Errores de usuarios
	EHI.5	Destrucción de la información
	EHI.6	Perdida de la información
	EHI.7	Sabotaje por personal propio de la organización.
	EHI.8	Secuestro, soborno o extorsión de un trabajador obligándole a cometer sabotajes en contra de su voluntad
	EHI.9	Incorrecta Manipulación de operaciones de sistema
	EHI.10	Incorrecta Manipulación de instalaciones de retención hidráulica
Fallos de los sistemas	EFS.1	Fallo persistente del sistema de operación
	EFS.2	Fallos persistentes del sistema de auscultación
	EFS.3	Fallos persistentes de los sistemas de seguridad

Tabla 18. Catálogo de Amenazas.