Especificaciones de ciberseguridad e integración de datos a implementar en las infraestructuras de la Agencia Balear del Agua y la Calidad Ambiental

v.2023/08

GOIB
CONSELLERIA DE LA MAR I DEL CICLE DE L'AIGUA
AGÈNCIA BALEAR AIGUA I QUALITAT AMBIENTAL

Palma, agosto de 2023

Tabla de Contenidos

1 Objetivo

El objetivo de este documento es el de definir las normas técnicas que deben implementarse en las infraestructuras de Saneamiento y Abastecimiento de la Agencia Balear del Agua y la Calidad Ambiental (en adelante, ABAQUA) para que sirvan de guía y/o ayuda a la hora de redactar los pliegos técnicos, desde el punto de vista de la explotación de datos y la ciberseguridad.

Este documento define, por un lado y de una forma general, la forma en que deben integrarse los datos de explotación de las instalaciones con el centro de procesamiento de datos de la ABAQUA, y por otra, las normas genéricas en materia de ciberseguridad que deben implementarse en las infraestructuras operadas por los explotadores.

2 Alcance de la especificación

Desde el punto de vista de la integración de los datos se definen los mecanismos que se han escogido para realizar la ingestión de los datos en el centro de procesamiento de datos de la ABAQUA.

Desde el punto de vista de la ciberseguridad, este documento define de forma genérica las zonas de seguridad que deben definirse, así como los protocolos que deben usarse para implementarlas.

3 Normativa de referencia

REF.	Descripción
IEC 62443	Conjunto de estándares sobre "Redes de comunicaciones industriales: seguridad informática para redes y sistemas". El estándar se divide en distintas secciones y describe aspectos tanto técnicos como relacionados con los procesos de la ciberseguridad industrial.
ISO 27001	Norma internacional sobre cómo gestionar la seguridad de la información.
ISO 22301	Estándar para la gestión de la continuidad de negocio.

4 Acrónimos

Acrónimos	Descripción
DMZ	Demilitarized Zone. Zona Desmilitarizada.
DC	Data Confidenciality. Confidencialidad del dato.
DoS	Denial Of Service. Denegación de Servicio.
FR	Foundational Requirements. Requisits primaris.
FW	Firewall. Cortafuegos
IAC	Identification & Authentication Controls. Controles de identificación y autentificación.
IT	Information Technology. Tecnologías de la información.
OT	Operational Technology. Tecnlologías operacionales.
RA	Resource Avalaibity. Disponibilidad del recurso.
RDF	Restricted DataFramework. Flujo de datos restringido.
RDP	Remote Desktop Protocol. Protocolo de escritorio remoto.
BCMS	Business Continuity Management System. Sistema de adminitración de la continuidad del negocio.
ISMS	Information Security Management System. Sistema de gestión de la seguridad de la información.
SI	System Integrity. Integridad del sistema.
SL	Security Level. Nivel de seguridad.
TRE	Time Response Event. Respuesta a evento en tiempo.
UC	Use Control. Control de uso.
DL	Data Lake. Repositorio centralitzado de datos.
REST	Representational State Transfer. REST es una arquitectura de software pensada para sistemas distribuidos basados en hipermedia, com la web.
API	Application Programming Interface. Interfície de aplicación programable.

5 Integración de los datos

Actualmente ABAQUA se encuentra en un proceso de digitalización que contempla, entre otros, la creación de un DL que contenga todos los datos que, de una forma u otro, forman parte del ámbito de negocio. Estos datos tienen, básicamente, tres orígenes.

I. Datos de explotación: Datos que provienen de las instalaciones o infraestructuras gestionadas por la ABAQUA (Caudalímetros, Sensores de pH, resultados de analíticas, ...)
II. Datos de gestión de las infraestructuras: Datos de las incidencias de las infraestructuras, ...
III. Datos de gestión de la ABAQUA: Información sobre las licitaciones, datos de los convenios, ...

Para definir cómo recoger la información referente al punto I. se ha puesto en marcha el proyecto Smart Water Islands. Para la definición de la recolección de los datos de los puntos II. y III. se han iniciado los trámites para desarrollar una Intranet para ABAQUA. En cualquiera de los tres casos, la información irá a parar a un DL que contendrá toda la información importante.

Este documento especifica las normas que deben implementarse desde el punto de vista de arquitectura IT en las infraestructuras para que esta recolección de datos se puedan llevar a cabo.

5.1 Tipos de instalaciones

Dada la heterogeneidad de las infraestructuras gestionadas, y con el objetivo de posibilitar la implementación de la recogida de los datos de explotación de forma segura se han definido los siguientes cuatro tipos de instalaciones en función del nivel de servicio del que debe disponer cada instalación.

Tipos	Descripción
1	Instalaciones que no hace falta que estén conectadas, pues no se monitorizan de forma remota.
2	Instalaciones que están conectadas de forma simple. No es necesaria la redundancia en las comunicaciones. Si falla la línea se perderán los datos.
3	Instalaciones que están conectadas de forma simple, pero sin pérdida de datos. Éstas se monitorizan como las anteriores, pero en caso de pérdida de las comunicaciones, los datos generados durante el período de no conexión se guardan localmente hasta que se restablezca la comunicación.
4	Instalaciones que deben estar conectadas de forma redundante. Son instalaciones vitales que siempre deben tener los datos disponibles. En caso de pérdida de una línea de comunicación, los datos se enviarán por una línea secundaria. Cuando la línea principal vuelva a estar disponible, volverán a enviar sus datos desde ésta sin necesidad de intervención humana. Sólo en caso de caída de las dos líneas a la vez se guardarán los datos localmente hasta el restablecimiento de la comunicación.

El proyecto Smart Water Islands define una arquitectura donde la entrada y salida de datos en el DL se realiza mediante una API, implementada con un servicio web REST, que se muestra en la figura 1.

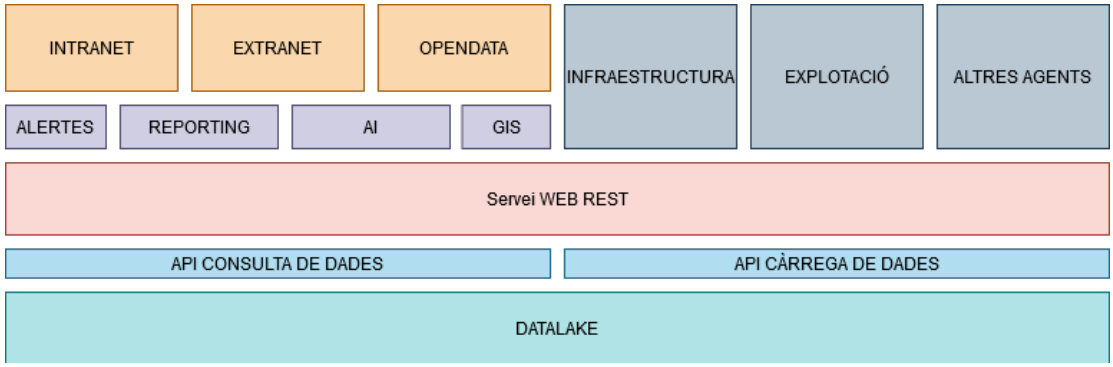

Figura 1. Arquitectura del proyecto Smart Water Islands.

La arquitectura final, incluyendo la red OT, queda de la siguiente forma:

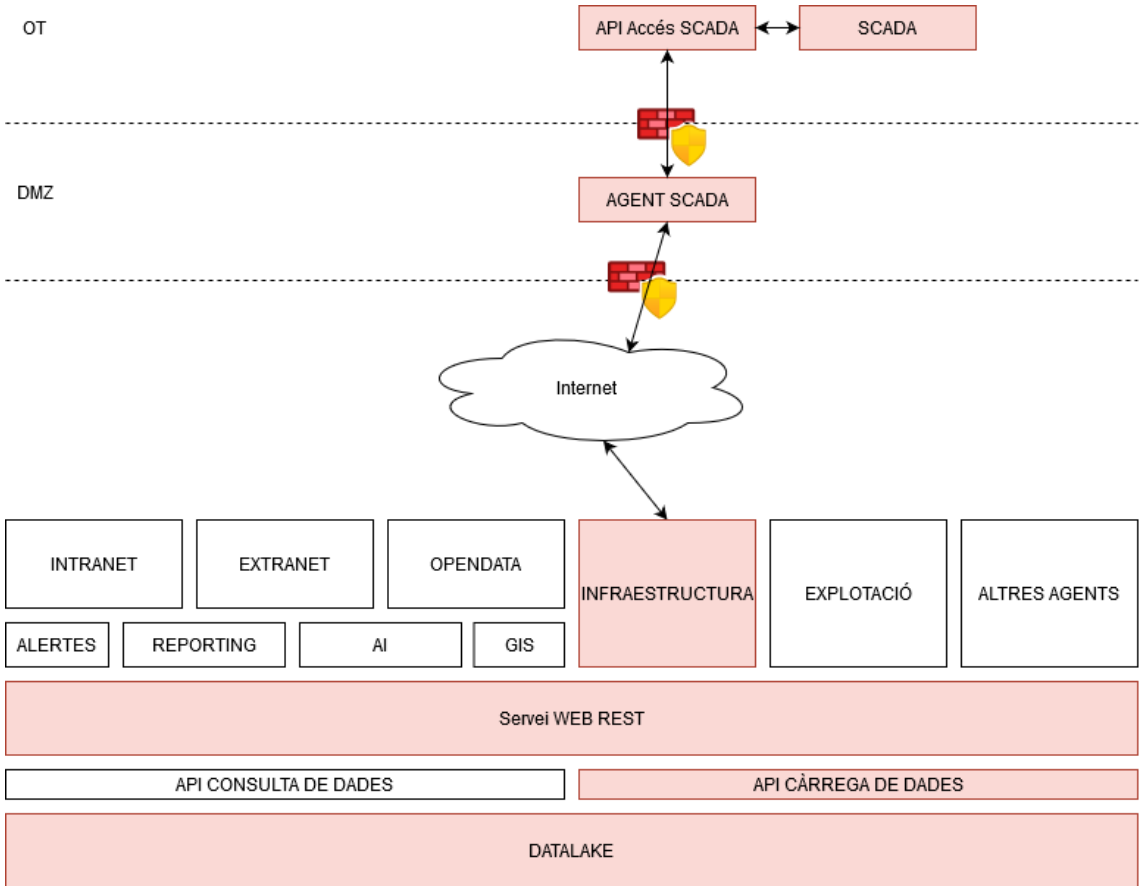

Figura 2. Arquitectura final incluyendo la red OT.

La comunicación de los datos entre el SCADA de la infraestructura y el DL de ABAQUA se realiza mediante un agente que será el encargado de leer los datos del histórico de la SCADA, a través de una API, y hacer su envío al DL.

Este agente no es responsabilidad del explotador, y en estos momentos se está diseñando. Lo que sí es responsabilidad del explotador es la de instalar una API para acceder a SCADA, tanto a los datos en vivo, como a los datos históricos. Actualmente todos los fabricantes de aplicaciones SCADA disponen de módulos para acceso a los datos de este. El coste de este módulo depende de cada fabricante.

Es importante que el módulo de acceso a los datos disponga de acceso tanto a los datos en vivo como a los datos históricos.

Además de los componentes anteriormente especificados, y en función de la categorización de la infraestructura en cuestión, se tendrán que provisionar las líneas de datos que sean necesarias, en base a la siguiente tabla.

Tipos	Número de líneas de datos i tipos
1	No es necesario ningún tipo de línea
2	Una única línea, siempre que posible, FFTH.
3	
4	Dos líneas, una línea principal y una secundaria. La principal ha de ser FFTH. De ser posible provisionar una segunda línea FFTH de un segundo proveedor, se elegirá un segundo proveedor.

Dado que la ubicación de las infraestructuras muchas veces no permite cumplir estas especificaciones, se aceptarán otras propuestas razonadas, y siempre que se hayan aceptado por parte del responsable de ABAQUA.

6 Ciberseguridad

Desde el punto de vista de la ciberseguridad, debe quedar claro que en ningún caso debe exponerse ningún componente de la red OT directamente en internet. Como se ha explicado en el punto anterior, lo que debe realizar el envío de los datos en modo PUSH debe ser el agente SCADA.

Se definen al menos dos zonas. La red OT y la DMZ. Estas dos redes estarán separadas y protegidas por dos FW.

Los FW tendrán que permitir una configuración en alta disponibilidad en modo ACTIVO-ACTIVO.

Las características mínimas de los componentes se definen en el punto 8 de este documento.

7 Coste de los componentes necesarios

Así pues, el listado de componentes que debe proveer el explotador para poder implementar esta arquitectura son los siguientes.

Partida			
Programa			
Componente		**Coste unitario**	**Total**
Módulo de acceso a los datos del SCADA		* €	* €
Módulo de histórico de los datos del SCADA		* €	* €
Programa SCADA		* €	* €
Hardware			
Componente	**Unidades**	**Coste unitario**	**Total**
Rack	1	1.500,00 €	1.500,00 €
Firewall	2	6.000.00 €	12.000,00 €

8 Descripción técnica de los componentes.

8.1 Firewall

Los dispositivos cortafuegos deben permitir la administración en la nube para facilitar su instalación y administración remota. Debe ofrecer un conjunto integral de servicios de red, para eliminar la necesidad de múltiples dispositivos.

Estos servicios deben ser, como mínimo, cortafuegos de aplicación de capa 7, filtrado de contenido, filtrado de búsqueda web, prevención de intrusiones basado en SNORT®, almacenamiento en caché web, WAN inteligente con múltiples enlaces ascendentes y conmutación por error 4G.

- **Hardware**
  - Rendimiento de cortafuegos con estado: 500 Mbps
  - Admitir aproximadamente hasta 200 usuarios
- **Gestión centralizada basada en la nube**
  - Gestionado centralmente a través de la web**.**
  - Clasifica aplicaciones, usuarios y dispositivos.
  - Implementaciones de autoabastecimiento sin contacto
- **Redes y Seguridad**
  - Cortafuegos con estado
  - VPN de aprovisionamiento automático site to site
  - Políticas basadas en identidad
  - VPN de cliente (IPsec)
  - Integración de directorio activo

8.2 Rack

- Altura de 42U a 47U
- Laterales desmontables
- Kit de unión incluidos
- Ruedas con frenos
- Entrada de cable de cepillo en techo y base
- Perfiles ajustables delanteros y traseros de 19 "
- Unidades marcadas en los perfiles
- 1000mm de fondo
- Puerta frontal con marco de cristal
- Puerta trasera de metal
- Color negro