

## **ZONA SISTEMA SIS**

### **1. Nivel de seguridad objetivo**

**NS-O = (2, 1, 0, 3, 1, 1, 4)**

NS-O = (IA, AU, IS, CD, RD, RE, DR)

- IA: Esquemas de identificación, autenticación y autorización
- AU: Esquemas de auditabilidad o control del uso de sistemas
- IS: Integridad del sistema
- CD: Confidencialidad de los datos
- RD: Restricciones en la transmisión de datos
- RE: Tiempo de respuesta a eventos
- DR: Disponibilidad de recursos

## 2. Escenarios evaluados

### 2.1 Esquemas de identificación, autenticación y autorización (IA)

ID	DESCRIPCIÓN DEL ESCENARIO	LÍM INF	LÍM SUP	PROB
1	Explotación de vulnerabilidades en conexiones remotas para acceso a la red de planta llevado a cabo por una empresa de la competencia	50.000,00 €	100.000,00 €	44 %
10	Explotación de vulnerabilidades al acceder al sistema SCADA por un ciberdelincuente	8.000,00 €	30.000,00 €	36 %

ID	COSTE MEDIDAS COMPENSATORIAS	EFFECTIVIDAD DE LAS MEDIDAS
1	5.000,00 €	10 %
10	5.000,00 €	10 %

### 2.2 Esquemas de auditabilidad o control del uso de sistemas (AU)

ID	DESCRIPCIÓN DEL ESCENARIO	LÍM INF	LÍM SUP	PROB
2	Modificación del software del SCADA llevado a cabo por un tercero encargado de realizar acciones de mantenimiento	20.000,00 €	60.000,00 €	46 %
11	Modificación de la configuración de PLC por un insider	30.000,00 €	60.000,00 €	23 %

ID	COSTE MEDIDAS COMPENSATORIAS	EFFECTIVIDAD DE LAS MEDIDAS
2		
11		

### 2.3 Integridad del sistema (IS)

ID	DESCRIPCIÓN DEL ESCENARIO	LÍM INF	LÍM SUP	PROB
----	---------------------------	---------	---------	------

3	Explotación de vulnerabilidades en el PLC de control al no estar correctamente parcheado llevado a cabo por un ciberdelincuente	25.000,00 €	70.000,00 €	20 %
8	Fallo en la actualización de lógica de control del PLC al no haberse probado correctamente el software durante su desarrollo	50.000,00 €	80.000,00 €	17 %

ID	COSTE MEDIDAS COMPENSATORIAS	EFFECTIVIDAD DE LAS MEDIDAS
3	6.000,00 €	18 %
8	6.000,00 €	18 %

#### 2.4 Confidencialidad de los datos (CD)

ID	DESCRIPCIÓN DEL ESCENARIO	LÍM INF	LÍM SUP	PROB
4	Brecha de datos sensible alojados en el servidor del histórico del sistema de control llevado a cabo por un ciberdelincuente	40.000,00 €	85.000,00 €	27 %
9	Brecha de datos de información relacionada con el diseño de detalle de planta alojada en servidores de ingeniería	20.000,00 €	60.000,00 €	67 %

ID	COSTE MEDIDAS COMPENSATORIAS	EFFECTIVIDAD DE LAS MEDIDAS
4		
9		

#### 2.5 Restricciones en la transmisión de datos (RD)

ID	DESCRIPCIÓN DEL ESCENARIO	LÍM INF	LÍM SUP	PROB
5	Acceso a la red de planta por un atacante al no estar el FW correctamente configurado	35.000,00 €	80.000,00 €	48 %

12	Acceso a la red de planta de un encargado de mantenimiento a través de conexión wifi	3.000,00 €	26.000,00 €	32 %
----	--	------------	-------------	------

ID	COSTE MEDIDAS COMPENSATORIAS	EFFECTIVIDAD DE LAS MEDIDAS
5	12.000,00 €	12 %
12	16.000,00 €	15 %

## 2.6 Tiempo de respuesta a eventos (RE)

ID	DESCRIPCIÓN DEL ESCENARIO	LÍM INF	LÍM SUP	PROB
6	Ransomware sobre SCADA producido por un ciberdelincuente	20.000,00 €	90.000,00 €	40 %
13	Fallo en la configuración PLC al no haberse seguido procediendos provoca una parada del proceso	10.000,00 €	50.000,00 €	20 %

ID	COSTE MEDIDAS COMPENSATORIAS	EFFECTIVIDAD DE LAS MEDIDAS
6	15.000,00 €	15 %
13	10.000,00 €	8 %

## 2.7 Disponibilidad de recursos (DR)

ID	DESCRIPCIÓN DEL ESCENARIO	LÍM INF	LÍM SUP	PROB
7	Ataque DDOS al SCADA de planta por un insider malicioso	30.000,00 €	95.000,00 €	47 %
14	Malware introducido a través de USB de PLC por un encargado de mantenimiento	11.000,00 €	90.000,00 €	53 %

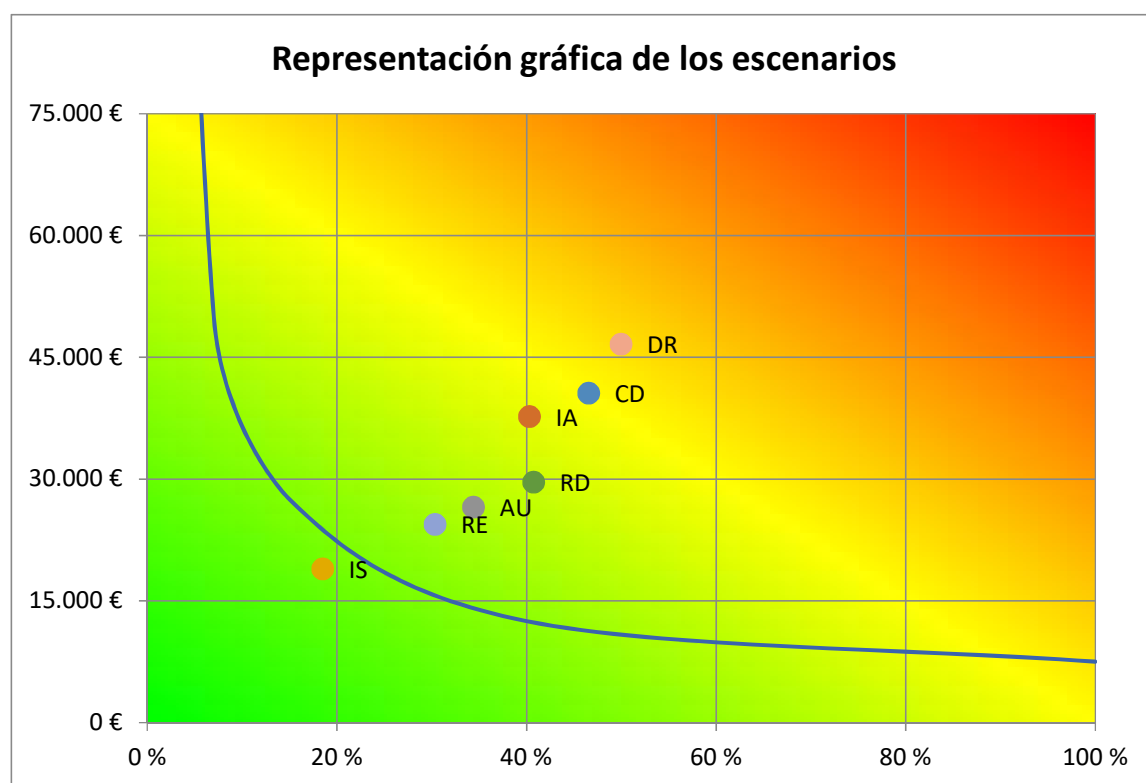
ID	COSTE MEDIDAS COMPENSATORIAS	EFFECTIVIDAD DE LAS MEDIDAS
----	------------------------------	-----------------------------

7	20.000,00 €	20 %
14	22.000,00 €	25 %

### 3. Valoración cuantitativa de los escenarios en cada dominio (Pérd. Inherente)

DOMINIO	PÉRDIDA MEDIA INHERENTE	PROB
Esquemas de identificación, autenticación y autorización (IA)	37.704 €	40 %
Esquemas de auditabilidad o control del uso de sistemas (AU)	26.539 €	34 %
Integridad del sistema (IS)	18.952 €	18 %
Confidencialidad de los datos (CD)	40.604 €	47 %
Restricciones en la transmisión de datos (RD)	29.643 €	41 %
Tiempo de respuesta a eventos (RE)	24.445 €	30 %
Disponibilidad de recursos (DR)	46.640 €	50 %

Nota: Valores obtenidos a partir de una simulación de 1500 iteraciones



#### 4. Valoración cuantitativa de los escenarios en cada dominio (Pérd. Residual)

DOMINIO	PÉRDIDA MEDIA RESIDUAL	PROB
Esquemas de identificación, autenticación y autorización (IA)	33.902 €	40 %
Esquemas de auditabilidad o control del uso de sistemas (AU)	N/A	34 %
Integridad del sistema (IS)	15.582 €	18 %
Confidencialidad de los datos (CD)	N/A	47 %
Restricciones en la transmisión de datos (RD)	25.985 €	41 %
Tiempo de respuesta a eventos (RE)	21.604 €	30 %
Disponibilidad de recursos (DR)	36.272 €	50 %

Nota: Valores obtenidos a partir de una simulación de 1500 iteraciones

## 5. Requisitos según la IEC-62443 asociados al Nivel de Seguridad Objetivo

### 5.1 Esquemas de identificación, autenticación y autorización (IA)

#### REQUISITOS

---

SR 1.1	Identificación y autenticación de usuarios personales
RE 1	Identificación y autenticación única
SR 1.2	Identificación y autenticación de procesos de software y dispositivos
SR 1.3	Gestión de cuentas
SR 1.4	Gestión de identificadores
SR 1.5	Gestión de autenticadores
SR 1.6	Gestión de accesos wireless
RE 1	Identificación y autenticación única
SR 1.7	Robustez de autenticación basada en contraseña
SR 1.8	Certificados de infraestructura de clave pública
SR 1.9	Robustez de autenticación de clave pública
SR 1.10	Respuesta del proceso de autenticación
SR 1.11	Intentos de login erróneos
SR 1.12	Notificación de uso del sistema
SR 1.13	Acceso a través de redes no confiables
RE 1	Acceso explícito requiere aprobación

### 5.2 Esquemas de auditabilidad o control del uso de sistemas (AU)

#### REQUISITOS

---

SR 2.1	Aplicación de la autorización
SR 2.2	Control de uso wireless
SR 2.3	Control de uso dispositivos de dispositivos portables y móviles
SR 2.4	Código móvil
SR 2.5	Bloqueo de sesión
SR 2.8	Eventos auditables
SR 2.9	Capacidad de almacenamiento de auditoría
SR 2.10	Respuesta a fallos de procesos de auditoría

### 5.3 Integridad del sistema (IS)

No aplican requisitos de ciberseguridad al ser el nivel de seguridad objetivo cero.

### 5.4 Confidencialidad de los datos (CD)

#### REQUISITOS

---

SR 4.1	Confidencialidad de la información
RE 1	Protección de la información en reposo o en tránsito a través de redes no confiables



SR 4.2	Persistencia de la información
RE 1	Purgado de recursos de memoria compartidos
SR 4.3	Uso de criptografía

## **5.5 Restricciones en la transmisión de datos (RD)**

### **REQUISITOS**

---

SR 5.1	Segmentación de red
SR 5.2	Protección de los límites de zona
SR 5.3	Restricciones de comunicación persona a persona por propósito general
SR 5.4	Particionado de aplicaciones

## **5.6 Tiempo de respuesta a eventos (RE)**

### **REQUISITOS**

---

SR 6.1	Accesibilidad a los log de auditoría
--------	--------------------------------------

## **5.7 Disponibilidad de recursos (DR)**

### **REQUISITOS**

---

SR 7.1	Protección contra la denegación de servicio
RE 1	Gestionar las cargas de comunicación
RE 2	Limitar efectos DoS a otros sistemas o redes
SR 7.2	Gestión de recursos
SR 7.3	Sistema de control de backup
RE 1	Verificación del backup
RE 2	Automatización del backup
SR 7.4	Recuperación y reconstitución del sistema de control
SR 7.5	Alimentación de emergencia
SR 7.6	Configuración de la red y de la seguridad
RE 1	Informe legible por máquina de la configuración de seguridad actual
SR 7.7	Menos funcionalidad
SR 7.8	Sistema de control de inventario de componentes