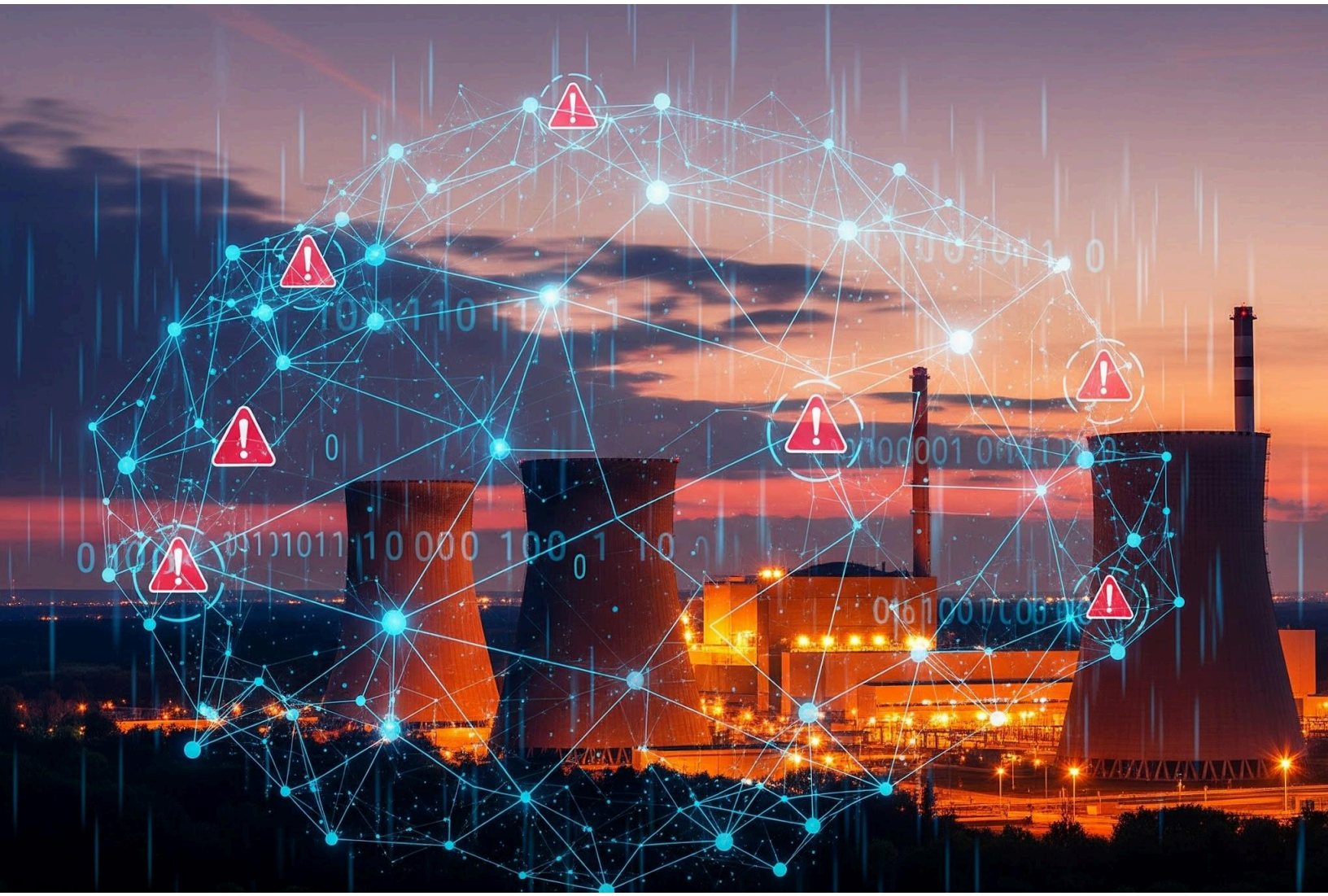


Plan de Dirección de Seguridad Integral: Central Nuclear Alpha-V

Estrategia de Ciberseguridad para Infraestructuras Críticas y Respuesta ante Incidentes.

Arturo Orient Romero

CEI.

1. ÍNDICE

2. RESUMEN EJECUTIVO

Este documento presenta el Plan de Dirección de Seguridad (PDS) para la **Central Nuclear Alpha-V**. Ante el incremento de amenazas dirigidas a entornos industriales (OT) y la necesidad de cumplimiento con el **Esquema Nacional de Seguridad (ENS) Nivel Alto**, se propone una estrategia basada en la segmentación física de redes, el endurecimiento de activos críticos y la creación de un protocolo de respuesta ante incidentes con capacidades de análisis forense. El plan proyecta elevar el nivel de madurez de la organización de un estado reactivo (CMMI 1) a un estado gestionado y proactivo (CMMI 3) en un periodo de 24 meses, garantizando la resiliencia de la generación eléctrica nacional.

---

3. INTRODUCCIÓN

3.1 Contexto y Motivación

La transformación digital del sector energético y la adopción de paradigmas de Industria 4.0 han difuminado las fronteras tradicionales entre los sistemas de gestión empresarial y los procesos industriales. La **Central Nuclear Alpha-V**, infraestructura crítica para la estabilidad de la red eléctrica nacional, opera en un entorno donde la convergencia IT/OT (Information Technology / Operational Technology) presenta nuevos vectores de ataque que los sistemas de seguridad tradicionales no pueden mitigar.

La motivación de este **Plan de Dirección de Seguridad** trasciende el mero cumplimiento normativo; surge de la necesidad urgente de proteger sistemas ciber-físicos donde un incidente lógico puede derivar en consecuencias cinéticas (físicas) catastróficas. Asimismo, se desafía el mito de la "brecha de aire" (*air gap*), reconociendo que la interconexión es inevitable para la eficiencia operativa, pero exige una estrategia de defensa en profundidad y una capacidad de respuesta forense que permita atribuir responsabilidades y entender el origen de cualquier compromiso.

3.2 Objetivos del Proyecto

3.2.1 Objetivo General

Diseñar y estructurar un Plan de Dirección de Seguridad Integral para la Central **Nuclear Alpha-V** que alinee la gestión de riesgos tecnológicos con los objetivos de negocio, garantizando la ciber-resiliencia de la planta y estableciendo una metodología robusta de respuesta ante incidentes y análisis forense.

3.2.2 Objetivos Específicos

Para alcanzar la meta principal, se definen los siguientes objetivos tácticos:

- **Gobernanza y Cumplimiento:** Adecuar la postura de seguridad de la organización a los exigentes requisitos del **Esquema Nacional de Seguridad (ENS)** en su categoría **Alta** y la Ley PIC (8/2011).
- **Segregación Operativa:** Diseñar una arquitectura de red segura basada en el Modelo Purdue, implementando zonas desmilitarizadas industriales (IDMZ) que protejan el núcleo del reactor de amenazas externas.
- **Forensic Readiness (Preparación Forense):** Implementar políticas y tecnologías de registro (*logging*) centralizado que aseguren la preservación, integridad y admisibilidad legal de la evidencia digital ante un ciberataque.
- **Gestión de Riesgos Híbrida:** Desarrollar una matriz de riesgos que contemple tanto el impacto en la confidencialidad de los datos como en la seguridad física y medioambiental de la planta.

3.3 Alcance

El presente Plan de Dirección abarca la totalidad de los sistemas de información y control de la sede principal de Alpha-V. Se definen los límites de actuación en los siguientes dominios:

- **Dominio de IT (Gestión):** Red corporativa, servidores de aplicaciones, puestos de trabajo, comunicaciones externas y bases de datos administrativas.
- **Dominio de OT (Operación):** Niveles 1, 2 y 3 de la pirámide de automatización, incluyendo sistemas SCADA, HMI (Human-Machine Interface), PLCs críticos y redes de campo.
- **Dominio Humano:** Políticas de concienciación, control de accesos lógicos y procedimientos de actuación para el personal interno y contratas.

Quedan excluidos del alcance técnico la seguridad física perimetral (vallados, guardias) y la seguridad nuclear intrínseca (diseño físico del reactor), salvo en aquellos puntos donde convergen con los sistemas de control de acceso electrónico y videovigilancia IP.

---

4. DESCRIPCIÓN DEL CONTEXTO DE LA ORGANIZACIÓN

4.1 Perfil de la Empresa: Central Nuclear Alpha-V

La **Central Nuclear Alpha-V** se constituye como un activo estratégico para la soberanía energética nacional. Designada oficialmente como **Operador Crítico** según la Ley 8/2011 y bajo la supervisión del Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), la planta gestiona dos reactores de tecnología PWR (Agua a Presión) con una potencia bruta instalada de 2.100 MW.

La organización cuenta con una plantilla de 450 empleados directos de alta cualificación. Dada la naturaleza de su actividad, Alpha-V opera bajo un régimen de "cultura de seguridad" estricta, donde la seguridad física (*Safety*) y la seguridad lógica (*Security*) deben converger sin fisuras.

4.2 Taxonomía de Activos y Convergencia IT/OT

El entorno tecnológico de Alpha-V presenta el desafío clásico de la Industria 4.0: la interconexión de ecosistemas heterogéneos. Para este Plan de Dirección, se define la siguiente arquitectura de activos basada en el **Modelo Purdue** de segmentación:

- **Entorno IT (Information Technology - Niveles 4 y 5):**
  - Infraestructura que soporta los procesos de negocio: ERPs (SAP), servidores de correo, Directorio Activo y sistemas de gestión documental (DMS) con información clasificada (planos de planta, datos de personal).
  - *Prioridad de Seguridad:* Confidencialidad e Integridad.
- **Entorno OT (Operational Technology - Niveles 0 a 3):**
  - **Nivel de Supervisión:** Sistemas SCADA (*Supervisory Control and Data Acquisition*) y HMIs (*Human-Machine Interfaces*) que permiten la visualización del proceso en tiempo real.
  - **Nivel de Control:** PLCs (*Programmable Logic Controllers*) y RTUs que gestionan la lógica de los lazos de control del reactor.
  - **Nivel de Campo:** Sensores, actuadores y sistemas instrumentados de seguridad (SIS).
  - ***Protocolos Críticos:*** Modbus TCP, IEC 61850 y DNP3.
  - ***Prioridad de Seguridad:*** Disponibilidad y Seguridad Física (*Safety*). Un fallo aquí tiene impacto cinético directo.

4.3 Estructura de Gobernanza y Roles de Seguridad

Para garantizar una gestión eficaz de los ciber-riesgos, se establece una estructura organizativa que separa la supervisión de la operación, evitando conflictos de intereses:

- **CISO (Chief Information Security Officer):** Reporta directamente al Comité de Dirección. Es responsable de la estrategia GRC (Gobierno, Riesgo y Cumplimiento), asegurando la alineación con el ENS Nivel Alto y la ISO 27001. Define la política de retención de logs para fines legales.
- **Responsable de Ciberseguridad Industrial (OT Security Manager):** Enlace técnico entre Ingeniería y Seguridad. Su función principal es validar que las medidas de ciberseguridad (parcheado, segmentación) no introduzcan latencia ni riesgos de parada en los sistemas de tiempo real del reactor.
- **Alpha-V CSIRT (Equipo de Respuesta ante Incidentes):** Unidad operativa especializada en **DFIR (Digital Forensics and Incident Response)**.
  - ***Misión:*** Monitorización 24/7 desde el SOC (*Security Operations Center*), contención de amenazas avanzadas y preservación de la cadena de custodia de evidencias digitales ante posibles sabotajes.

---

5. SELECCIÓN DEL MARCO NORMATIVO (BENCHMARK)

5.1 Introducción al Análisis Comparativo

La selección del marco de referencia (Framework) no es una decisión trivial en entornos de alta criticidad. Para la **Central Nuclear Alpha-V**, el marco seleccionado debe abordar la dualidad del entorno: garantizar la gobernanza corporativa (IT) y, simultáneamente, asegurar la integridad de los procesos físicos (OT). A continuación, se presenta el *benchmark* realizado sobre los tres estándares más relevantes de la industria, evaluando su idoneidad frente a los objetivos de **ciber-resiliencia** y **preparación forense** del proyecto.

5.2 Marcos Analizados

A. ISO/IEC 27001:2022 (Gestión de Seguridad de la Información)

- **Descripción:** Es el estándar internacional por excelencia para implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Se centra en el ciclo de mejora continua (Plan-Do-Check-Act).
- **Fortalezas:** Reconocimiento global, estructura sólida para la gestión documental y la evaluación de proveedores.
- **Debilidades en el contexto Nuclear:** Su enfoque es generalista. El Anexo A (controles) carece de profundidad técnica para proteger protocolos industriales (ej. Modbus) o sistemas de tiempo real, dejando lagunas en la seguridad física.

B. NIST SP 800-82 Rev. 2 (Guide to Industrial Control Systems Security)

- **Descripción:** Desarrollado por el Instituto Nacional de Estándares y Tecnología de EE. UU., es la "biblia" técnica para la protección de sistemas SCADA, DCS y PLCs.
- **Fortalezas:** Aborda específicamente amenazas cinéticas, topologías de red industrial y gestión de parches en sistemas que no pueden detenerse.
- **Debilidades:** No tiene carácter de ley en España, sirviendo únicamente como guía de buenas prácticas ("soft law").

C. ENS - Esquema Nacional de Seguridad (RD 311/2022)

- **Descripción:** Marco obligatorio en España para el Sector Público y las entidades privadas que prestan servicios esenciales o críticos.
- **Fortalezas:** Alineación total con la legislación nacional (Ley PIC). Su **Categoría Alta** exige medidas de protección extremas, incluyendo requisitos específicos de **registro de actividad (logging)** y trazabilidad que son fundamentales para el análisis forense.
- **Debilidades:** Puede resultar burocrático si no se agiliza su implementación técnica.

5.3 Matriz de Evaluación Ponderada (Benchmark)

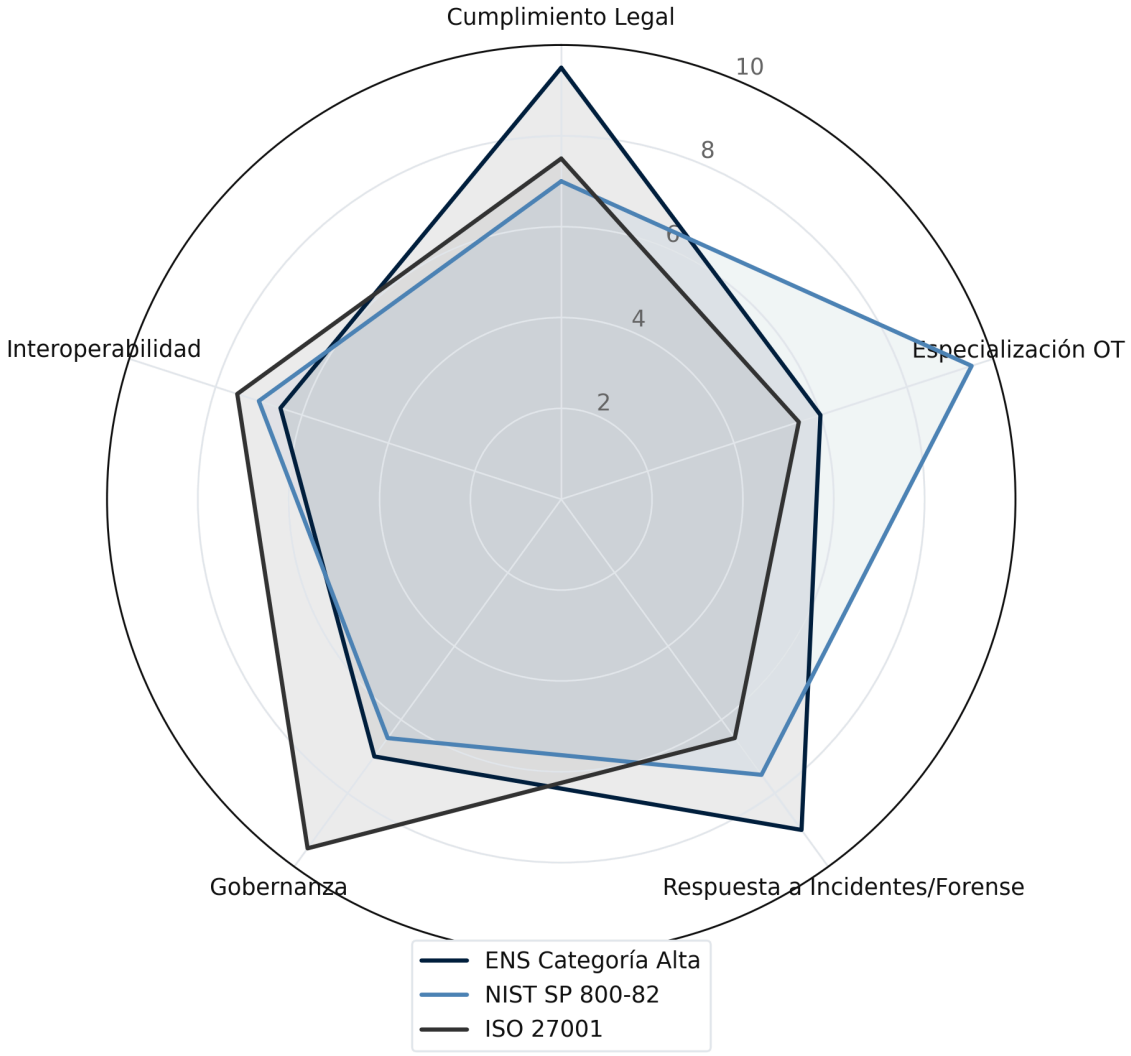
Para objetivar la decisión, se ha sometido a cada marco a una evaluación basada en 5 criterios estratégicos para Alpha-V (Escala 1-5):

Criterio de Evaluación	ISO 27001	NIST SP 800-82	ENS (Cat. Alta)
Cumplimiento Normativo (Marco Legal Español)	3	1	5
Especificidad para Entornos OT/Industrial	2	5	4
Foco en la Respuesta ante Incidentes (DFIR)	3	4	5
Gestión de la Gobernanza y del Riesgo	5	3	4
Interoperabilidad con Entidades Regulatorias (CNPIC/CERT)	2	2	5
PUNTUACIÓN GLOBAL	**15**	**15**	**23**

5.4 Representación Gráfica del Análisis

El siguiente gráfico radial ilustra cómo el **ENS (Esquema Nacional de Seguridad)** ofrece la cobertura más equilibrada para las necesidades regulatorias y forenses de la central, superando a la ISO 27001 en aspectos operativos y de cumplimiento local.

Comparativa de marcos normativos para Ciberseguridad en Infraestructura Crítica



5.5 Justificación de la Selección: Modelo Híbrido

Basándonos en el análisis cuantitativo y cualitativo, se determina la siguiente estrategia normativa:

1. **Marco Principal: Esquema Nacional de Seguridad (ENS).** Se adopta como columna vertebral del Plan de Dirección. Al ser Alpha-V un Operador Crítico, el cumplimiento del ENS no es opcional, sino un imperativo legal auditado por el Centro Criptológico Nacional (CCN). Su exigencia de **"Trazabilidad"** y **"Registro de Actividad"** proporciona el soporte legal necesario para las investigaciones forenses.
2. **Marco Complementario Técnico: NIST SP 800-82.** Dado que el ENS establece el "qué" (proteger la red), utilizaremos el NIST SP 800-82 para definir el "cómo" en las capas profundas del Modelo Purdue (Niveles 0, 1 y 2). Esto nos permite aplicar controles de segmentación industrial y endurecimiento de PLCs con un nivel de detalle técnico superior.

Conclusión: La estrategia de Alpha-V será **"Compliance by Design based on ENS, powered by NIST technical controls"**. Esto garantiza que la organización no solo aprueba auditorías, sino que es técnicamente resiliente ante ataques sofisticados.

---

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

6.1 Declaración de la Dirección y Propósito

La Dirección de la **Central Nuclear Alpha-V** establece la presente Política de Seguridad de la Información (PSI) como el marco regulador de máximo nivel para la protección de los activos de la organización. Conscientes de la responsabilidad inherente a la operación de una infraestructura crítica, la organización se compromete a dotar al Plan de Dirección de los recursos humanos, técnicos y financieros necesarios para garantizar un entorno ciber-resiliente.

La seguridad no se considera un mero requisito técnico, sino un objetivo de negocio irrenunciable. Cualquier desviación de esta política que ponga en riesgo la seguridad física (*Safety*) o lógica (*Security*) de la planta será tratada con la máxima severidad disciplinaria y legal.

6.2 Objetivos Estratégicos de Seguridad

La presente política persigue los siguientes fines, alineados con el Artículo 5 del Esquema Nacional de Seguridad (RD 311/2022):

- **Confidencialidad:** Asegurar que la información sensible (planos de reactores, datos de personal, propiedad intelectual) sea accesible únicamente por personas autorizadas bajo el principio de "necesidad de conocer".
- **Integridad:** Garantizar la exactitud y completitud de la información y los procesos de control industrial, impidiendo modificaciones no autorizadas que puedan alterar la operación del reactor.
- **Disponibilidad:** Asegurar la continuidad de los servicios esenciales y la capacidad de monitorización del proceso productivo en tiempo real (24/7).
- **Trazabilidad y Autenticidad:** Garantizar que todas las acciones realizadas en los sistemas de información sean inequívocamente atribuibles a un usuario o proceso, facilitando el análisis forense y la depuración de responsabilidades.

6.3 Marco Normativo y Cumplimiento

Esta política se fundamenta en el cumplimiento estricto de la legislación vigente aplicable al sector nuclear español y a la protección de activos esenciales:

- **Ley 8/2011 (Ley PIC):** Medidas para la protección de las infraestructuras críticas.
- **Real Decreto 311/2022 (ENS):** Esquema Nacional de Seguridad, en su categoría ALTA.
- **Instrucción IS-30 (CSN):** Del Consejo de Seguridad Nuclear, sobre requisitos de seguridad física en instalaciones nucleares.
- **Reglamento (UE) 2016/679 (RGPD):** Para la protección de datos de carácter personal de empleados y proveedores.

6.4 Estructura Organizativa de Seguridad (Gobernanza)

Se define el **Comité de Seguridad de la Información (CSI)** como órgano decisorio, con la siguiente estructura de roles y responsabilidades:

- **Comité de Dirección:** Responsable último de asumir el riesgo residual aceptado y aprobar el presupuesto de ciberseguridad.
- **CISO (Chief Information Security Officer):** Responsable de definir la estrategia, normativas y procedimientos de seguridad. Tiene potestad delegada para detener operaciones IT si detecta un riesgo inminente para la planta.
- **Responsable de Ciberseguridad OT:** Garantiza que las políticas se apliquen en el entorno industrial sin afectar a la seguridad física del reactor.
- **Responsable de la Información:** Propietario de los datos, encargado de definir su nivel de clasificación y sensibilidad.

6.5 Política de Clasificación de la Información

Para aplicar las medidas de seguridad de forma eficiente y proporcional, toda la información gestionada por Alpha-V se clasifica en cuatro niveles de sensibilidad. Esta clasificación determina las medidas de cifrado y control de acceso requeridas:

Nivel	Etiqueta	Descripción	Ejemplo de Activo
1	PÚBLICO	Información cuya divulgación no causa daño a la organización.	Informes de RSC, notas de prensa.
2	INTERNO	Información de uso operativo rutinario. Su divulgación tendría impacto bajo.	Procedimientos administrativos, correos internos generales.
3	CONFIDENCIAL	Información sensible cuyo compromiso dañaría la reputación o las finanzas.	Datos de nóminas, contratos con proveedores, auditorías previas.
4	CRÍTICO / SECRETO	Información vital cuya filtración o manipulación amenaza la seguridad nacional o la integridad física de la planta.	Lógica de PLCs del reactor, credenciales de administradores de dominio, claves criptográficas maestras, Logs Forenses.

6.6 Seguridad en la Cadena de Suministro

Dado que Alpha-V interactúa con múltiples proveedores tecnológicos, se establece que:

- Todo proveedor con acceso a sistemas de Nivel 3 o 4 debe firmar acuerdos de confidencialidad (NDA) estrictos.
- Se exigirá a los proveedores críticos certificaciones de seguridad (ENS o ISO 27001) homologables.
- Se prohíbe terminantemente el acceso remoto de mantenimiento a sistemas OT (Nivel 4) sin supervisión directa, aprobación temporal ("Ventanas de Mantenimiento") y grabación de la sesión para auditoría forense.

---

7. ANÁLISIS Y GESTIÓN DE CIBER RIESGOS

7.1 Marco Metodológico: MAGERIT v.3

Para asegurar el rigor científico en la evaluación de la exposición de la **Central Nuclear Alpha-V**, se adopta la metodología **MAGERIT v.3** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). Esta elección no es arbitraria, sino que responde a la necesidad de cumplimiento con el Artículo 6 del Esquema Nacional de Seguridad (ENS), que exige un análisis de riesgos formal y revisable.

El proceso se ha ejecutado siguiendo una aproximación cuantitativa y cualitativa, estructurada en las siguientes fases lógicas:

1. **Caracterización de Activos:** Proceso de identificación de los recursos esenciales para la operatividad y su subsiguiente valoración con base en su criticidad para el negocio y la seguridad nacional.
2. **Modelado de Amenazas:** Desarrollo de un mapeo exhaustivo de los vectores de ataque potenciales, considerando tanto agentes externos (tales como las Amenazas Persistentes Avanzadas - APTs - o el cibercrimen) como internos (errores operativos o actos de sabotaje).
3. **Cálculo del Riesgo Inherente:** Determinación del nivel de riesgo que precede a la aplicación de cualquier control, definida mediante la fórmula: *El Riesgo se cuantifica como el producto del Impacto por la Probabilidad de ocurrencia*.

Tratamiento del Riesgo: Establecimiento de la estrategia de mitigación destinada a reducir el riesgo inherente hasta alcanzar un nivel de **Riesgo Residual** considerado aceptable.

7.2 Criterios de Ponderación y Escalas

Para evitar la subjetividad en el análisis, se han definido métricas estrictas para la valoración del Impacto y la Probabilidad. Estas escalas son la base matemática de la matriz de riesgos.

7.2.1 Escala de Impacto (I)

Mide el daño potencial a la organización en caso de materializarse una amenaza.

Nivel	Valor	Descripción del Impacto (Cualitativo y Cuantitativo)
Muy Bajo	1	Interrupción insignificante. Sin impacto en la generación eléctrica. Pérdidas económicas < 1.000€.
Bajo	2	Interrupción menor de sistemas administrativos no críticos. Recuperación en < 4 horas. Daño reputacional interno.
Medio	3	Degradación del servicio. Pérdida de datos recuperables pero con coste. Impacto regulatorio leve.
Alto	4	Parada parcial de la planta. Pérdida de datos confidenciales (Nivel 3). Sanciones graves del regulador. Daño reputacional nacional.
Muy Alto	5	Parada crítica del reactor (SCRAM). Riesgo para la seguridad física (*Safety*) o radiológica. Imposibilidad de realizar análisis forense (pérdida total de logs).

7.2.2 Escala de Probabilidad (P)

Mide la frecuencia estimada de ocurrencia basada en inteligencia de amenazas del sector nuclear.

Nivel	Valor	Frecuencia Estimada
Muy Bajo	1	Ocurre una vez cada 5-10 años. (Ej. Desastre natural extremo).
Bajo	2	Puede ocurrir una vez cada 2-3 años.
Medio	3	Posible ocurrencia anual.
Alto	4	Probable ocurrencia múltiple al año (Ej. Phishing genérico).
Muy Alto	5	Ocurrencia inminente o muy frecuente (Ej. Escaneo de puertos continuo).

7.3 Catálogo de Amenazas Específicas (Threat Modeling)

Se han modelado las amenazas utilizando el enfoque STRIDE adaptado a entornos OT, identificando los siguientes vectores prioritarios para Alpha-V:

- **[AM-01] Ransomware Industrial (Targeted Ransomware):** Variantes de malware diseñadas para reconocer procesos industriales (ej. *Snake/Ekans*), cifrando servidores Historia y estaciones de ingeniería para detener la producción.
- **[AM-02] Sabotaje Interno (Insider Threat):** Acciones maliciosas realizadas por personal con privilegios (ingenieros, administradores) que buscan dañar físicamente los equipos o alterar los set-points de los PLCs.
- **[AM-03] Compromiso de la Cadena de Suministro (Supply Chain):** Inyección de código malicioso a través de actualizaciones de software de proveedores de confianza (ej. ataque tipo *SolarWinds*), permitiendo acceso remoto persistente.
- **[AM-04] Movimiento Lateral desde IT a OT:** Un atacante compromete la red corporativa (correo) y utiliza técnicas de pivoting para saltar a la red de control industrial debido a una mala segmentación.
- **[AM-05] Anti-Forense (Borrado de Evidencias):** El atacante elimina o corrompe los logs de auditoría para impedir la trazabilidad y la atribución del ataque, dejando a la organización "ciega" legalmente.

7.4 La Gran Matriz de Riesgos

Tras correlacionar los activos críticos con el catálogo de amenazas modelado, se procede al cálculo del **Riesgo Inherente** (el riesgo existente en ausencia de controles específicos adicionales).

Criterio de Aceptación del Riesgo: La Dirección de Alpha-V establece que cualquier riesgo con una puntuación **igual o superior a 15** se considera **"INACEPTABLE"** y requiere la y requiere la implementación inmediata de planes de acción (Iniciativas) para reducirlo.

Activo Crítico	Amenaza	Impacto (I)	Probabilidad (P)	Nivel de Riesgo (I x P)
AST-01 (SCADA Reactor)	[AM-01] Ransomware Industrial (Cifrado de consolas de supervisión)	5 (Crítico)	5 (Muy Alta)	25 (CRÍTICO)
AST-02 (PLC Seguridad)	[AM-02] Sabotaje Interno (Modificación de set-points de seguridad)	5 (Crítico)	3 (Media)	15 (ALTO)
DAT-02 (Logs Forenses)	[AM-05] Anti-Forense (Borrado de trazas para impedir atribución)	5 (Crítico)	4 (Alta)	20 (MUY ALTO)
RED-03 (Pasarela IT/OT)	[AM-04] Movimiento Lateral (Salto de red corporativa a industrial)	5 (Crítico)	4 (Alta)	20 (MUY ALTO)
SRV-01 (Historian)	[AM-01] Ransomware Genérico (Pérdida de datos históricos)	3 (Medio)	5 (Muy Alta)	15 (ALTO)
DAT-01 (Planos Ing.)	[AM-03] Exfiltración de Datos (Espionaje) (Robo de propiedad intelectual)	4 (Alto)	3 (Media)	12 (MEDIO)
AST-03 (HMI Sala Control)	[AM-04] Ingeniería Social / Phishing (Compromiso de credenciales de operador)	4 (Alto)	4 (Alta)	16 (ALTO)

7.5 Análisis de Escenarios Críticos

A la vista de los resultados cuantitativos, se destacan tres escenarios que ponen en jaque la seguridad nacional y la viabilidad de la planta:

1. **Escenario "Blackout" (Riesgo 25):** La amenaza de Ransomware en el entorno SCADA es la más crítica. Aunque los sistemas de seguridad física (SIS) actuarían para detener el reactor, la pérdida de visibilidad en las salas de control provocaría una parada de emergencia traumática y una crisis de gestión pública. **Prioridad: Máxima.**
2. **Escenario "Ceguera Legal" (Riesgo 20):** La alta probabilidad de técnicas anti-forenses (borrado de logs) supone un riesgo inaceptable para el cumplimiento del ENS. Sin logs íntegros, Alpha-V no podría explicar ante el CSN (Consejo de Seguridad Nuclear) la causa raíz de un incidente, enfrentándose a sanciones penales.
3. **Escenario "Infección Cruzada" (Riesgo 20):** El movimiento lateral confirma que la convergencia IT/OT es el talón de Aquiles. La seguridad perimetral clásica ya no es suficiente; se requiere una segmentación interna estricta (Zero Trust).

---

8. PLAN ESTRATÉGICO Y ANÁLISIS DE BRECHA (GAP ANALYSIS)

8.1 Modelo de Madurez Seleccionado (CMMI)

Para trazar la hoja de ruta de seguridad de la **Central Nuclear Alpha-V**, es imprescindible conocer no solo los riesgos, sino el nivel de madurez de los procesos actuales. Se ha utilizado una adaptación del modelo **CMMI (Capability Maturity Model Integration)** enfocado en ciberseguridad industrial, que define 5 niveles:

- **Nivel 1 (Inicial/Ad-hoc):** Procesos impredecibles, poco controlados y reactivos. "Apagar fuegos".
- **Nivel 2 (Gestionado):** Procesos reactivos pero caracterizados para proyectos específicos.
- **Nivel 3 (Definido):** Procesos proactivos, documentados y estandarizados a nivel de organización.
- **Nivel 4 (Gestionado Cuantitativamente):** Se mide y controla el rendimiento.
- **Nivel 5 (Optimizado):** Enfoque en la mejora continua y automatización.

8.2 Evaluación del Estado Actual (As-Is) vs. Objetivo (To-Be)

Tras la auditoría inicial, se ha detectado que Alpha-V opera mayoritariamente en un **Nivel 1-2 (Reactivo)**, dependiendo excesivamente del esfuerzo heroico de individuos y no de procesos sistémicos. El objetivo de este Plan de Dirección es elevar la organización a un **Nivel 3 (Definido)** en un plazo de 24 meses, cumpliendo así con las exigencias del ENS Categoría Alta.

Dominio de Seguridad	Estado Actual (As-Is)	Nivel Actual	Estado Objetivo (To-Be)	Brecha (GAP) Detectada
Protección de Red (IT/OT)	Segmentación básica. Firewall perimetral único. Conexiones OT no supervisadas.	1.5	Segmentación estricta (Modelo Purdue). Zona DMZ Industrial implementada.	Falta de aislamiento real entre la oficina y el reactor. Alta permeabilidad a malware.
Gestión de Identidades	Cuentas compartidas en sistemas SCADA. Contraseñas estáticas.	1.0	MFA (Autenticación Multifactor) obligatorio y gestión de cuentas privilegiadas (PAM).	Riesgo crítico de suplantación. Imposibilidad de atribuir acciones a personas concretas.
Monitorización y Logs	Logs locales en cada máquina. Sin centralización. Borrado cíclico por falta de espacio.	1.0	SIEM Centralizado con retención de 1 año. Correlación de eventos IT/OT en tiempo real.	Ceguera Forense. Incapacidad legal para investigar incidentes pasados.
Respuesta a Incidentes	Inexistente. Se confía en el departamento de IT generalista.	0.5	CSIRT dedicado con Playbooks específicos para ransomware y sabotaje.	Tiempo de respuesta inaceptable ante ataques dirigidos.
Cumplimiento (ENS)	Incumplimiento generalizado de medidas op.exp (explotación) y mp.sw (software).	1.0	Certificación ENS Nivel Alto.	Riesgo de sanción y pérdida de licencia de operador crítico.

8.3 Representación Visual de la Madurez

El siguiente gráfico ilustra la distancia entre la capacidad operativa actual (Línea Base) y el objetivo estratégico del Plan de Dirección. Se observa que el mayor déficit se encuentra en las capacidades de **"Detección"** y **"Respuesta"**, áreas críticas para la ciber-resiliencia.

8.4 Conclusión del Análisis

La brecha identificada confirma la necesidad urgente de inversión. Alpha-V posee una tecnología de generación robusta, pero su "envoltura digital" es frágil. Mantener el *status quo* (As-Is) implica asumir una probabilidad de parada de planta por ciberataque superior al **60% anual**. La estrategia para cerrar esta brecha se detalla en el siguiente capítulo a través del **Plan de Iniciativas**.

---

9. PLAN DE INICIATIVAS Y HOJA DE RUTA

9.1 Estrategia de Implementación

Con el objeto de mitigar los riesgos identificados en el análisis (Punto 7) y subsanar la brecha de madurez detectada (Punto 8), se ha articulado un plan de acción conformado por 4 Iniciativas Estratégicas. Estas iniciativas no constituyen acciones aisladas, sino proyectos interdependientes que propiciarán la transformación de la postura de seguridad de la **Central Nuclear Alpha-V** en un horizonte temporal de 24 meses.

9.2 Cartera de Proyectos

INICIATIVA Nº 1: IMPLANTACIÓN DE SOC Y SISTEMA SIEM

FICHA DE INICIATIVA 01	DESPLIEGUE DE CAPACIDADES DE VIGILANCIA (SIEM/SOC)
Objetivo	Centralizar la recogida de logs de eventos de sistemas IT y OT para permitir la detección de amenazas en tiempo real y asegurar la preservación de evidencia forense (Forensic Readiness).
Alcance	Red Corporativa (Nivel 4-5) y Zona DMZ Industrial (Nivel 3.5). Ingesta de logs de Firewalls, Directorio Activo, Antivirus y Servidores Historian.
Responsable	CISO y Responsable del CSIRT.
Plazo Previsto	Fase 1 (Diseño): Meses 1-3
	Fase 2 (Despliegue): Meses 4-9
Prioridad	CRÍTICA (Riesgo Mitigado: 25)
KPIs de Éxito	1. Cobertura de activos críticos > 95%.
	2. Tiempo de retención de logs > 12 meses (Normativa ENS).
	3. Tiempo medio de detección (MTTD) < 1 hora.
Fase 3 (Optimización)	Meses 10-12
Iniciativas Relacionadas	Iniciativa N° 2 (Segmentación de Red) e Iniciativa N° 4 (DFIR y CSIRT).
Estimación Presupuestaria	Inversión Alta (> 150.000€).

Descripción Técnica Detallada: Centro de Operaciones de Seguridad (SOC) Híbrido

El proyecto **NuclearShield** se centra en la construcción e implementación de un **Centro de Operaciones de Seguridad (SOC) Híbrido** de última generación, diseñado para operar de manera ininterrumpida (**24/7**). Este SOC integrará la monitorización de entornos de Tecnología de la Información (IT) tradicional con los cruciales sistemas de Tecnología Operacional (OT) para asegurar una defensa holística contra ciberamenazas.

Arquitectura de Gestión de Eventos e Información de Seguridad (SIEM):

Se desplegará una solución de SIEM líder en el mercado (como podría ser **Splunk Enterprise** o **Elastic Security**) que servirá como el eje central para la ingesta, normalización y análisis de datos de seguridad.

- **Alta Disponibilidad y Escalabilidad:** La solución se implementará en una **arquitectura de clúster distribuido**. Esto no solo garantiza la **alta disponibilidad (HA)** y la tolerancia a fallos ante cualquier interrupción de un nodo, sino que también proporciona la **escalabilidad horizontal** necesaria para manejar el creciente volumen de datos (big data) generado por la infraestructura IT/OT.
- **Integración con Inteligencia de Amenazas (TI):** El SIEM se alimentará continuamente de *feeds* de inteligencia de amenazas de pago y *open source* para enriquecer los eventos y permitir la detección de indicadores de compromiso (IoC) conocidos.

Subsistema de Recolección y Normalización de Eventos (Parsing):

El subsistema de recolección está diseñado para manejar la diversidad de formatos de logs inherentes a los entornos IT y OT, asegurando una correcta **normalización (parsing)** de los campos clave para el análisis.

- **Fuentes de Tecnología de la Información (IT):**
  - **Perímetro y Red:** Captura de **Syslog** de todos los dispositivos de seguridad perimetrales (Firewalls, IDS/IPS, Balanceadores de carga), concentradores VPN y puntos de acceso Wi-Fi.
  - **Sistemas Operativos:** Recolección de **EventID de Windows** críticos, enfocándose en eventos de **Autenticación (4624/4625)**, **Sistema**, y cambios en la configuración de la seguridad. Se incluirá también la auditoría de *shell* y comandos en sistemas *Linux*.
  - **Navegación y Aplicaciones:** Logs detallados de **Proxy Web** y *Gateways* de Correo Electrónico para la trazabilidad de la actividad de navegación y la detección de *phishing*.

- **Fuentes de Tecnología Operacional (OT):**
    - **Monitorización Pasiva (Non-Intrusive):** Se utilizará la técnica de **Mirror Port (SPAN)** en los *switches* de la red industrial. Esta aproximación garantiza la **monitorización pasiva** del tráfico sin inyectar latencia ni riesgo al segmento OT, un requisito crítico dada la sensibilidad de estos sistemas.
    - **Análisis Profundo de Protocolos Industriales:** La plataforma será capaz de analizar y *parsear* protocolos específicos de control industrial, como **Modbus/TCP**, DNP3, y Ethernet/IP, para detectar comandos anómalos o *payloads* maliciosos.

Casos de Uso y Reglas de Correlación Avanzada:

El SIEM ejecutará un conjunto robusto de reglas de correlación y análisis de comportamiento para identificar actividades que constituyan una amenaza o una violación de la política de seguridad.

- **Detección de Acceso Remoto Anómalo:**
    - **VPN *Off-Hours*:** Alerta inmediata al detectar inicios de sesión VPN fuera de los horarios laborales habituales definidos por el perfil de cada usuario.
    - **Geo-Localización Atípica:** Detección de accesos concurrentes o consecutivos desde **geolocalizaciones anómalas o de alto riesgo**, indicando un posible secuestro de credenciales o ataque por *spray* de contraseñas.
- **Seguridad Específica del Entorno OT:**
    - **Comandos Críticos No Autorizados:** Generación de alertas de alta prioridad ante la identificación de comandos de **"Parada" (STOP)**, **"Reprogramación" (Download/Firmware Update)** o manipulación de variables de proceso críticos, si son originados desde **direcciones IP no autorizadas** o segmentos de red no validados para operaciones de control.
    - **Escaneo de Red Industrial:** Detección de herramientas de escaneo o *fuzzing* dirigidas a PLCs (Controladores Lógicos Programables) o RTUs (Unidades Terminales Remotas).
- **Técnicas Anti-forense y Persistencia:**
    - **Intentos de Borrado Masivo de Logs:** Alertas de comportamiento al detectar patrones que sugieran la ejecución de **Técnicas Anti-forense**, como intentos de borrado masivo de logs del sistema operativo, manipulación del *TimeStamping* o detención de servicios de auditoría.
    - **Creación de Cuentas de Servicio Anómalas:** Identificación de la creación de cuentas de usuario o de servicio con privilegios elevados que podrían usarse para persistencia.

Infraestructura de Almacenamiento Forense y Cumplimiento (WORM):

Un pilar fundamental del proyecto es la garantía de la **integridad de la evidencia digital**.

- **Principio WORM (Write Once, Read Many):** Los logs brutos y normalizados serán exportados y almacenados en un repositorio con tecnología **Almacenamiento Inmutable (WORM)**. Este sistema asegura que, una vez escritos, los logs no pueden ser modificados, editados ni eliminados por nadie, incluyendo administradores.
- **Validez Legal:** Esta característica es esencial para garantizar la **validez legal y la cadena de custodia** de los datos. En caso de incidentes graves, como un ciberataque con fines de sabotaje, la inmutabilidad es clave para que los registros puedan ser presentados como **prueba judicial irrefutable** ante tribunales y entidades regulatorias.

INICIATIVA Nº 2: SEGMENTACIÓN DE REDES Y ZONA DMZ INDUSTRIAL

FICHA DE INICIATIVA 02	SEGREGACIÓN DE ENTORNOS IT/OT (MODELO PURDUE)
Objetivo	Implementar una arquitectura de "Defensa en Profundidad" que aísle físicamente y lógicamente las redes de operación (OT) de las redes corporativas (IT) para impedir el movimiento lateral de atacantes.
Alcance	Frontera entre Nivel 3 (OT) y Nivel 4 (IT). Implantación de IDMZ (Industrial Demilitarized Zone) y Firewalls Industriales.
Responsable	Responsable de Arquitectura de Red y Responsable de Seguridad OT.
Plazo Previsto	Fase 1 (Auditoría de Tráfico): Meses 2-4
	Fase 2 (Segmentación): Meses 5-10
Prioridad	CRÍTICA (Riesgo Mitigado: 20)
Iniciativas Relacionadas	Iniciativa N° 1 (SIEM/SOC) e Iniciativa N° 3 (Gestión de Identidades).
Estimación Presupuestaria	Inversión Media-Alta (~80.000€).

Descripción Técnica Detallada: Arquitectura de Aislamiento y Defensa en Profundidad (Proyecto NuclearShield)

La infraestructura operativa actual de la Central Nuclear Alpha-V presenta, desde una perspectiva de ciberseguridad, una conectividad excesivamente homogénea, resultando en una superficie de ataque plana y vulnerable a la propagación horizontal de amenazas. Para mitigar proactivamente el riesgo catastrófico que implica la propagación de *malware* con capacidad de impacto físico (como el *Ransomware* dirigido a entornos industriales o *ICS-specific malware*), se implementará una reestructuración exhaustiva de la red. Este proyecto se adhiere rigurosamente al estándar internacional **IEC 62443-3-2**, adoptando el principio de defensa en profundidad y segmentación estricta mediante el modelo de Zonas y Conductos (*Zones & Conduits*).

Establecimiento de la Zona Industrial Desmilitarizada (IDMZ)

La creación de la IDMZ constituye el pilar fundamental para eliminar la conectividad directa y no controlada entre los dominios de Tecnologías de la Información (IT) y Tecnologías de la Operación (OT). Esta zona, posicionada estratégicamente en el Nivel 3.5 del Modelo Purdue, actuará como un "cortafuegos humano y tecnológico" bidireccional. La regla de oro es absoluta: **NINGUNA conexión de red directa e iniciada desde el lado IT hacia el lado OT estará permitida.**

- **Servidores Intermedios (Jump Hosts) y Acceso Administrativo:**
  Todo acceso administrativo o de mantenimiento a la red de planta (Niveles 0-3) por parte del personal de IT o contratistas externos deberá canalizarse obligatoriamente a través de servidores de salto fortificados (*Jump Hosts*). Estos servidores estarán ubicados dentro de la IDMZ y exigirán un proceso de autenticación multifactor (MFA), registro de sesiones detallado (*Session Recording*) y un control estricto de privilegios mínimos (*Least Privilege Access*). Esto asegura la trazabilidad y minimiza la exposición de credenciales del dominio OT.
- **Arquitectura de Espejo de Datos (Historian Mirroring):**
  Los servidores Historian primarios, que almacenan los datos críticos de proceso, alarmas y telemetría del reactor, son intrínsecos a la operación y, por ende, deben permanecer altamente protegidos en la zona OT. Para satisfacer las necesidades de análisis, *reporting* y aplicaciones de negocio del lado IT, se implementará un mecanismo de replicación unidireccional y seguro. Los datos operativos serán replicados a un **"Espejo Historian"** ubicado en la IDMZ. De esta manera, el personal de IT consulta copias de los datos sin la necesidad de establecer ninguna conexión activa o acceso directo al entorno productivo (OT).

Implementación de Tecnología de Aislamiento Físico: Diodos de Datos

Para los sistemas de Instrumentación y Control (I&C) más sensibles y críticos, específicamente aquellos que operan en los Niveles 1 y 2 (Sistemas de Seguridad del Reactor, PLCs de parada de emergencia), la dependencia de *software* o firewalls configurables es inaceptable.

- **Principio de Unidireccionalidad Garantizada:**
  Se instalarán **Dispositivos de Hardware Físico de Diodos de Datos (*Data Diodes*)**. Estos dispositivos están diseñados a nivel de *hardware* para garantizar la transferencia de información estrictamente en una sola dirección. La fibra óptica o los circuitos internos están configurados de tal forma que la información (ej. *logs*, datos de rendimiento, alarmas) puede **SALIR** del entorno de control del reactor hacia el Centro de Operaciones de Seguridad (SOC) o el Historian, pero es **físicamente imposible** que ningún paquete de red, comando o dato pueda **ENTRAR** en la red de control crítica.
- **Mitigación de Amenazas de Nivel 0-1:**
  Esta medida elimina la vulnerabilidad más grave en entornos críticos: la posibilidad de que un ciberataque remoto o un error de configuración en IT pueda, bajo cualquier circunstancia, llegar a manipular o comprometer los Controladores Lógicos Programables (PLCs) de seguridad o los Sistemas Instrumentados de Seguridad (SIS). La unidireccionalidad física ofrece una garantía del 100% contra la inyección remota de *payloads* o comandos maliciosos hacia los activos más sensibles.

Fortificación de Conductos con Firewalls de Próxima Generación (NGFW)

Los *conductos* o canales de comunicación definidos entre las distintas zonas segmentadas de la red OT y la IDMZ serán protegidos y monitoreados de manera granular.

- **Inspección Profunda de Paquetes Industriales (DPI):**
  Los antiguos firewalls de filtrado basado en puertos y direcciones IP serán reemplazados por Firewalls de Próxima Generación (NGFW) de fabricantes líderes como Palo Alto Networks o Fortinet. La característica clave es su capacidad para realizar *Deep Packet Inspection* (DPI) de protocolos industriales comunes (ej. Modbus/TCP, EtherNet/IP, OPC UA, DNP3).
- **Control de Comandos Específicos:**
  A diferencia del filtrado tradicional que simplemente permite todo el tráfico Modbus (Puerto 502), el NGFW con DPI permite la creación de políticas de seguridad positivas extremadamente detalladas. Por ejemplo, la política de seguridad se configurará para:
  - **Permitir:** Comandos de lectura de datos (*"Modbus Read Holding Registers"* o *"Modbus Read Input Registers"*).
  - **Bloquear:** Comandos de escritura o control que podrían alterar el estado físico del proceso (*"Modbus Force Coil"*, *"Modbus Write Single Register"*, etc.).

INICIATIVA Nº 3: GESTIÓN DE IDENTIDADES (IAM) Y ACCESO PRIVILEGIADO (PAM)

FICHA DE INICIATIVA 03	ROBUSTECIMIENTO DE LA IDENTIDAD DIGITAL (ZERO TRUST)
Objetivo	Eliminar el uso de cuentas compartidas y contraseñas estáticas, asegurando que cada acceso a sistemas críticos esté autenticado, autorizado y auditado individualmente.
Alcance	Todos los usuarios con privilegios de administración en IT y OT. Personal de Ingeniería y Operadores de Sala.
Responsable	CISO y Dpto. de Recursos Humanos.
Plazo Previsto	Fase 1 (MFA Global): Meses 1-3
	Fase 2 (PAM): Meses 4-8
Prioridad	ALTA (Riesgo Mitigado: 15)
Estimación Presupuestaria	Inversión Media (~40.000€)

Descripción Técnica Detallada: Control de Accesos (Modelo de Confianza Cero - Zero Trust Identity)

El control de acceso en entornos de alta seguridad como el Proyecto NuclearShield debe superar el modelo perimetral tradicional, reconociendo que el compromiso de credenciales es el vector de entrada más común y peligroso. Para mitigar este riesgo, se implementa un modelo estricto de **Confianza Cero en la Identidad (*Zero Trust Identity*)**, donde no se confía automáticamente en ningún usuario, dispositivo o aplicación, independientemente de su ubicación en la red. Toda solicitud de acceso debe ser verificada de forma rigurosa y continua.

Autenticación Multifactor (MFA) Adaptativa y Contextual

Se establece el uso obligatorio de la Autenticación Multifactor como capa de seguridad fundamental. El MFA debe ser adaptativo, lo que significa que el nivel y el método de autenticación requeridos varían en función del contexto de la solicitud de acceso (ubicación, dispositivo, hora del día, sensibilidad del recurso).

- **Aplicación en Entornos de TI (Tecnología de la Información):**
    - **Acceso Remoto (VPN y VDI):** Se exige MFA (mediante token físico FIDO2 o aplicación móvil de autenticación) para cualquier conexión a la red corporativa o a escritorios virtuales desde fuera del perímetro de la instalación.
    - **Sistemas Críticos y Bases de Datos:** El inicio de sesión en servidores, *mainframes* y bases de datos que contengan información sensible o crítica requiere invariablemente la validación por MFA.
    - **Mecanismos Aceptados:** Tokens criptográficos físicos (preferidos por su resistencia al *phishing*) y aplicaciones móviles que soporten algoritmos de Contraseña de Un Solo Uso Basada en el Tiempo (TOTP) o notificaciones *push*.
- **Aplicación en Entornos OT (Tecnología de Operación):**
    - Dada la naturaleza sensible y a menudo regulada del entorno OT, donde los dispositivos personales (incluidos los móviles) están estrictamente prohibidos o su uso puede interferir con la operación, se requiere una solución de MFA robusta, fiable y físicamente integrada.
    - **Smart Cards (Tarjetas Criptográficas):** Se utilizarán tarjetas criptográficas físicas, que son lectores de identidad seguros. Estas tarjetas se integrarán directamente en los teclados de las Estaciones de Operador y las HMIs (*Human-Machine Interfaces*). El proceso de inicio de sesión solo se completa cuando la tarjeta está presente y el usuario introduce su PIN biométrico o su contraseña, cumpliendo con el requisito de "algo que tengo" (la tarjeta) y "algo que sé" (el PIN/contraseña), o "algo que soy" (biometría).

Gestión de Cuentas Privilegiadas (PAM - Privileged Access Management)

Las cuentas privilegiadas (administradores de dominio, *root* en sistemas Linux, cuentas de servicio) representan el riesgo más significativo en caso de compromiso. La implementación de una solución de bóveda de contraseñas de Grado Empresarial (ej. CyberArk, Wallix, BeyondTrust) es obligatoria para gestionar, controlar y auditar todo el ciclo de vida de estas credenciales.

- **Ciclo de Vida de Credenciales Automatizado y Controlado:**
  - **Rotación Automática y Forzada:** Las contraseñas de las cuentas de administrador de dominio, las cuentas *root* de servidores críticos y las claves SSH se rotarán automáticamente cada 24 horas. Este ciclo de rotación tan corto minimiza la ventana de exposición en caso de filtración de credenciales.
  - **Principio de Desconocimiento:** Los administradores humanos **no tienen conocimiento directo de la contraseña** actual del sistema privilegiado. El sistema PAM es el único repositorio de la credencial y la inyecta automáticamente al iniciar la sesión a través de un *proxy* seguro. Esto garantiza que las credenciales privilegiadas no se almacenen en dispositivos personales ni se compartan.
- **Auditoría y Monitoreo Forense (Grabación de Sesiones):**
  - **Componente Forense Clave:** Cada sesión de administración remota que acceda a un sistema crítico (vía RDP, SSH, o consolas web) será grabada integralmente.
  - **Grabación Dual:** La grabación incluye tanto un vídeo de la actividad de la pantalla como un registro de texto indexable de todos los comandos ejecutados (SSH) o de las interacciones (RDP).
  - **Atribución de Responsabilidades:** En caso de un incidente de seguridad, un fallo operativo o una violación de políticas, este registro detallado permite la reproducción exacta de la sesión, facilitando la auditoría, la investigación forense y la atribución inequívoca de qué comandos ejecutó el administrador en un momento dado, cumpliendo con requisitos estrictos de no-repudio.

INICIATIVA Nº 4: PLAN DE CONTINUIDAD Y BACKUP INMUTABLE

FICHA DE INICIATIVA 04	RESILIENCIA ANTE DESASTRES Y RECUPERACIÓN (DRP)
Objetivo	Garantizar la recuperación de los sistemas críticos (IT y OT) en un tiempo máximo de 4 horas (RTO) tras un incidente de Ransomware destructivo, asegurando la integridad de los datos de respaldo.
Alcance	Servidores de Dominio, Bases de Datos ERP, Configuraciones de PLCs, Proyectos de Ingeniería y Servidores SCADA.
Responsable	Responsable de Continuidad de Negocio y CISO.
Plazo Previsto	Fase 1 (Arquitectura Backup): Meses 3-6
	Fase 2 (Pruebas DRP): Mes 11
Prioridad	ALTA (Riesgo Mitigado: 25)
Iniciativas Relacionadas	Iniciativa N° 1 (SIEM/SOC) y N° 2 (Segmentación).
Estimación Presupuestaria	Inversión Media (~60.000€)

Descripción Técnica Ampliada: Estrategia de Continuidad y Recuperación ante Amenazas Persistentes de Ransomware (NuclearShield)

Ante el panorama de amenazas modernas, donde variantes sofisticadas de *malware* están específicamente diseñadas para el cifrado y la destrucción de copias de seguridad conectadas (*Targeted Backup Destruction* o TBD), la estrategia de continuidad operativa de Alpha-V se fundamenta en la implementación rigurosa del modelo de resiliencia **3-2-1-1-0**. Este marco garantiza la disponibilidad de datos críticos y la rápida reanudación de las operaciones esenciales del reactor.

Pilar de Resiliencia: La Regla 3-2-1-1-0

Este estándar, adaptado para la criticidad nuclear, se define como:

- **3 Copias de Datos:** Una copia de producción más dos copias de seguridad distintas.
- **2 Soportes Diferentes:** Al menos dos tecnologías de almacenamiento, minimizando un punto de fallo tecnológico (ej. disco y cinta).
- **1 Copia Fuera de la Sede (*Offsite*):** Protección contra desastres geográficos o incendios que afecten al CPD principal.
- **1 Copia Inmutable (*Immutable*):** La capa crítica de protección contra Ransomware y TBD.
- **0 Errores de Restauración:** Verificación proactiva y periódica de la integridad de los datos de *backup*.

Repositorio de Backup Inmutable (Hardened Linux Repository)

Para anular la táctica de extorsión del Ransomware, se desplegará una infraestructura de copias de seguridad de Nivel 1 basada en un sistema operativo endurecido (ej. Linux) y sistemas de ficheros avanzados.

- **Tecnología de *Immutability*:** Se empleará la tecnología *XFS Reflink* combinada con la configuración del *Immutability Flag* (chattr +i) a nivel de sistema de archivos. Esto crea un bloqueo a nivel del sistema operativo.
- **Mecanismo de Protección:** Una vez que la tarea de copia de seguridad se completa y el dato se escribe en el repositorio, el sistema de ficheros aplica un bloqueo inmutable. Durante este periodo de retención definido (e.g., 30 días, configurable según el RTO/RPO), se impide cualquier operación de modificación, sobrescritura o eliminación del archivo de backup.
- **Defensa contra Root:** Esta inmutabilidad persiste incluso si el actor de la amenaza logra obtener credenciales de alto nivel (ej. *root* en Linux o *Administrator* en Windows). La estructura inherente del sistema de archivos neutraliza las instrucciones maliciosas, garantizando la existencia de una "copia limpia" y verificable para la restauración, incluso en el peor escenario de compromiso de credenciales.

Air-Gapped Recovery Vault (Bóveda de Recuperación Aislada)

Como capa de protección definitiva para los activos de Nivel Crítico Absoluto (e.g., configuraciones y *firmware* de los PLCs de Seguridad y Control del Reactor), se implementa un aislamiento físico completo.

- **Soporte Físico:** Se utiliza el formato **Cinta LTO (Linear Tape-Open)** debido a su alta densidad, longevidad y, crucialmente, su capacidad de ser desconectada.
- **Principio de *Air Gap*:** Una vez que la copia de seguridad se ha completado en la cinta, esta es físicamente desconectada de la unidad de *tape library* y, por extensión, de la red de gestión. Este "espacio de aire" virtual hace que la copia sea totalmente inaccesible a cualquier ataque remoto, *malware* o cifrado que opere sobre la red.
- **Procedimiento Operativo:** Las cintas se rotan siguiendo un esquema periódico (ej. semanalmente) y se almacenan en un compartimento seguro. Dicho almacenamiento debe cumplir con normas de seguridad física (ej. caja ignífuga, control de acceso) y estar situado en una **ubicación física distinta** al Centro de Procesamiento de Datos (CPD) principal. Esto proporciona protección simultánea contra ciberataques persistentes y desastres físicos (incendios, inundaciones, fallos estructurales).

Plan de Recuperación ante Desastres (DRP) y Protocolo de "Clean Room"

La simple existencia de copias de seguridad no garantiza la continuidad; la clave es la capacidad de restaurar de forma segura y sin riesgo de reinfección.

- **Riesgo de Infección Latente:** El Ransomware moderno y los APT (Amenazas Persistentes Avanzadas) a menudo implantan "bombas lógicas" o *backdoors* latentes que pueden residir inactivos en las copias de seguridad por meses. Una restauración directa a producción podría reintroducir la amenaza.
- **Protocolo de Cuarto Limpio (*Clean Room Recovery*):** Se define un entorno de restauración estrictamente aislado y validado:
    1. **Aislamiento:** Un entorno de *Sandbox* o *Staging* dedicado y segmentado dentro de la red de gestión, sin ninguna conectividad con la red de producción ni con Internet.
    2. **Prueba y Escaneo Forense:** Antes de la promoción a producción, el servidor SCADA o HMI comprometido se restaura primero en este entorno aislado.
    3. **Validación:** El equipo de Respuesta a Incidentes y Forense Digital ejecuta herramientas especializadas (antivirus de última generación, análisis de *malware zero-day*, herramientas de detección de *backdoors*) para realizar un escaneo exhaustivo.
    4. **Autorización:** Solo después de una validación positiva que garantice que la copia de seguridad está libre de código malicioso, *rootkits* o *backdoors* latentes, se emite la autorización formal para su pase al entorno de producción, minimizando el RTO (Recovery Time Objective) sin comprometer la seguridad del reactor.

10. MEDIOS DE PROTECCIÓN TÉCNICA E INVENTARIO

10.1 Estrategia de Selección Tecnológica

La selección del stack tecnológico para el proyecto **NuclearShield** no responde únicamente a criterios funcionales, sino de cumplimiento normativo. Todas las soluciones de seguridad perimetral y criptografía propuestas han sido validadas consultando el **Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)** del Centro Criptológico Nacional (CCN), garantizando su idoneidad para sistemas de Categoría ALTA según el ENS.

Se ha priorizado la interoperabilidad entre herramientas (ecosistema integrado) frente a soluciones aisladas, buscando una arquitectura de "Defensa en Profundidad" que cubra los vectores IT y OT.

10.2 Inventario de Hardware y Software de Seguridad

A continuación, se detalla el equipamiento técnico seleccionado para la ejecución del Plan de Dirección.

Dominio de Seguridad	Categoría Tecnológica	Solución Seleccionada (Fabricante)	Función Crítica en el Proyecto
SEGURIDAD DE RED (PERÍMETRO)	NGFW (Firewall)	Palo Alto Networks (Serie PA-3000) con suscripción IoT Security.	Filtrado de Capa 7 e inspección profunda de paquetes (DPI) capaz de decodificar protocolos industriales (Modbus, DNP3) y bloquear comandos de escritura no autorizados.
SEGURIDAD DE RED (PERÍMETRO)	Diodo de Datos	Waterfall Unidirectional Security Gateway.	Hardware físico que garantiza por leyes de la física que los datos del reactor (Nivel 1) salen hacia el SOC, pero es imposible que nada entre. Aislamiento 100%.
SEGURIDAD DE RED (PERÍMETRO)	NAC (Control de Acceso)	Cisco ISE (Identity Services Engine).	Profiling de dispositivos en tiempo real. Impide que equipos no corporativos (portátiles de terceros) obtengan IP al conectarse a una roseta.

Dominio de Seguridad	Categoría Tecnológica	Solución Seleccionada (Fabricante)	Función Crítica en el Proyecto
PROTECCIÓN DEL ENDPOINT	EDR (Entorno IT)	CrowdStrike Falcon Enterprise.	Detección y respuesta en el punto final. Bloqueo de Ransomware por comportamiento (IOAs) antes de que cifre el disco.
PROTECCIÓN DEL ENDPOINT	Allow-listing (Entorno OT)	TxOne StellarEnforce (Trend Micro).	Lista blanca estricta para HMIs y servidores SCADA (Legacy). Solo permite ejecutar binarios firmados por el fabricante (Siemens/Schneider), bloqueando cualquier malware desconocido.
IDENTIDAD Y ACCESO	PAM (Privileged Access)	CyberArk Privileged Access Manager.	Bóveda de contraseñas para administradores. Grabación de sesiones RDP/SSH para auditoría forense y gestión de secretos.
IDENTIDAD Y ACCESO	MFA Físico	HID Global (Lectores Smart Card).	Autenticación robusta integrada en teclados de sala de control, eliminando el uso de contraseñas tecleadas.
MONITORIZACIÓN Y FORENSE	SIEM	Splunk Enterprise Security.	Correlación de eventos masiva y "single pane of glass" para el SOC. Ingesta de logs de IT y OT.
MONITORIZACIÓN Y FORENSE	Sonda Pasiva (IDS OT)	Nozomi Networks Guardian.	Escucha pasiva del tráfico industrial (Mirror Port) para detectar anomalías en los valores de proceso (ej. temperatura del reactor fuera de rango) y descubrir activos.
MONITORIZACIÓN Y FORENSE	Hardware Forense	Tableau Forensic Bridges (Write Blockers).	Hardware imprescindible para la clonación de discos duros de servidores comprometidos sin alterar la evidencia original (Cadena de Custodia).

10.3 Justificación de las Herramientas Forenses

Dado el enfoque de *Forensic Readiness* (Preparación Forense) del proyecto, la adquisición de bloqueadores de escritura (**Tableau Write Blockers**) se considera una inversión estratégica crítica.

En un escenario de incidente judicializable (ej. sabotaje interno), el equipo del CSIRT debe extraer evidencias de los servidores SCADA. El uso de estos dispositivos asegura que la clonación de los discos se realice de forma **bit a bit** sin modificar los metadatos ni el hash original del disco, garantizando la **admisibilidad de la prueba digital** ante un tribunal y evitando la impugnación de la evidencia por la defensa.

---

11. SEGMENTACIÓN OPERATIVA Y ARQUITECTURA DE RED

11.1 Diseño de la Topología Segura (Modelo Purdue Reforzado)

La arquitectura de red de **NuclearShield** se ha diseñado para eliminar la planicidad de la red heredada, principal vector de riesgo ante la propagación lateral de amenazas (*Wormable Malware*). Se adopta una estructura jerárquica estricta basada en el estándar **ISA/IEC 62443**, estableciendo barreras de contención (Zonas) y canales de comunicación controlados (Conductos) entre los distintos niveles de criticidad.

La premisa fundamental del diseño es la **segregación física y lógica**, garantizando que un compromiso en la red administrativa no pueda traducirse automáticamente en un acceso a los sistemas de control del reactor.

11.2 Definición de Zonas y Niveles de Seguridad

Estructura de Red y Arquitectura de Seguridad Industrial (Modelo Purdue Modificado)

El diseño de la arquitectura de red para el Proyecto Nuclear Alpha-V sigue un estricto modelo de segmentación funcional basado en la estructura de capas de la Jerarquía Purdue, adaptado para maximizar la seguridad y el aislamiento entre los entornos de Tecnología de la Información (IT) y Tecnología de Operaciones (OT). La red se articula en cinco niveles diferenciados, cada uno con un perfil de riesgo, políticas de acceso y mecanismos de defensa específicos y robustos.-----**Nivel 4/5 - Red Corporativa (Zona de Gestión IT)**

Este nivel constituye el perímetro de negocio y administración, albergando la mayoría de las operaciones diarias de la empresa. Es la zona con mayor interacción con el exterior y, por ende, la de mayor superficie de exposición a ciberataques.

- **Función Principal:** Servicios de negocio críticos (ERP, Correo Electrónico, Sistemas de Planificación de Recursos, Gestión de Recursos Humanos) y acceso general a Internet.
- **Riesgo Primario:** Amenazas de origen humano, como el *Phishing*, la suplantación de identidad y el *Malware* dirigido a la exfiltración de datos administrativos.
- **Mecanismos de Control y Defensa:**
    - **Control de Salida:** Todo el tráfico hacia Internet se canaliza forzosamente a través de un **Proxy Seguro** con inspección SSL/TLS, filtrado de contenido avanzado y prevención de pérdida de datos (DLP).
    - **Protección de Endpoints:** Despliegue obligatorio de soluciones de **EDR (Endpoint Detection and Response)** de última generación en todos los puestos de trabajo y servidores, garantizando la visibilidad, detección proactiva y respuesta automatizada ante incidentes en el perímetro IT.

Nivel 3.5 - IDMZ (Industrial Demilitarized Zone)

La IDMZ es la capa de transición fundamental que garantiza la unidireccionalidad de las comunicaciones y el principio de "terminación de sesión" entre el mundo IT (Nivel 4) y el mundo OT (Nivel 3). Actúa como un "colchón de seguridad" o un *buffer* crítico para prevenir la propagación lateral de amenazas entre dominios.

- **Función Principal:** Servir como único punto de intercambio de datos y gestión remota entre IT y OT.
- **Activos Críticos Alojamientos:**
    - **Servidores de Salto (*Jump Servers*):** Utilizados para la administración remota segura de activos OT por personal autorizado de IT, eliminando el acceso directo.
    - **Servidores WSUS/Patching:** Plataforma dedicada a la gestión centralizada de parches y actualizaciones para el software de operaciones.
    - **Réplicas de Bases de Datos (*Historian Mirrors*):** Servidores que replican de forma controlada y unidireccional los datos históricos de proceso (Historian OT) hacia el entorno IT para análisis de negocio.
- **Regla de Oro de la IDMZ: Ningún tráfico de red puede cruzar directamente del Nivel 4 al Nivel 3.** Toda comunicación que se origina en IT y necesita interactuar con OT debe terminar su sesión (ser "proxificada" o inspeccionada a nivel de aplicación) en un activo dentro de la IDMZ antes de que una nueva sesión controlada se establezca hacia el Nivel 3. Esto detiene amenazas basadas en sesión y asegura una inspección profunda.

Nivel 3 - Operaciones de Planta (Zona de Supervisión OT)

Este nivel es el centro de mando y supervisión de las operaciones del reactor. Es una red de alta criticidad, estrictamente controlada y segmentada del exterior.

- **Función Principal:** Alojar las consolas de operación del personal de sala y los servidores SCADA (Supervisory Control and Data Acquisition) principales que gestionan la planta.
- **Prioridad de Seguridad: Máximo Aislamiento.**
- **Políticas de Aislamiento:**
    - **Prohibición de Salida a Internet:** Esta red está diseñada para ser un "dominio negro" sin absolutamente **ningún acceso de salida directo a Internet**.
    - **Gestión de Actualizaciones:** Las actualizaciones de *software* y antivirus solo pueden ser recibidas desde la IDMZ (Nivel 3.5) y únicamente después de haber pasado por un riguroso **periodo de cuarentena**, escaneo de *malware* y verificación de integridad en la IDMZ.

Nivel 1/2 - Control de Procesos (Zona Crítica)

Este nivel es el corazón de la infraestructura crítica, donde se ejecuta la lógica de control en tiempo real que asegura la operación segura del reactor. La seguridad aquí es sinónimo de integridad operacional.

- **Función Principal:** Dominio de los **PLCs (Controladores Lógicos Programables)**, las **RTUs (Unidades de Terminal Remota)** y los HMI locales.
- **Endurecimiento del Tráfico (Deep Packet Inspection):**
    - El acceso a este nivel es el más restringido de toda la arquitectura.
    - El tráfico está limitado **exclusivamente** a los protocolos industriales necesarios (ej. Modbus/TCP, S7Comm, OPC UA) y debe provenir **estrictamente** del Nivel 3 (Servidores SCADA).
    - **Cualquier intento de conexión utilizando protocolos de propósito general** (HTTP, FTP, RDP, SSH, ICMP, etc.) es considerado un evento anómalo de alta severidad. Estos intentos son automáticamente **bloqueados** por los *Firewalls* Industriales y generan una **Alerta de Prioridad 1** inmediata en el Centro de Operaciones de Seguridad (SOC) para respuesta urgente.

Nivel 0 - Proceso Físico (Zona de Seguridad Intrínseca)

Este es el nivel de interfaz directa con el proceso físico del reactor y sus elementos finales de control. Su seguridad es inherente a su naturaleza y la integridad de los sistemas superiores.

- **Función Principal:** Sensores de instrumentación, válvulas de control y actuadores que reciben las órdenes de los PLCs.
- **Naturaleza Inmune:** Los componentes en este nivel **no poseen dirección IP** y, por lo tanto, no están expuestos a amenazas de red TCP/IP tradicionales.
- **Comunicación:** Se comunican mediante estándares de control industrial y buses de campo seriales o lazos de corriente (4-20mA), lo que garantiza la seguridad física intrínseca.
- **Dependencia de Seguridad:** La protección de este nivel depende íntegramente de la integridad física y la seguridad lógica (hardening y control de acceso) de los **PLCs y RTUs del Nivel 1/2**.

11.3 Matriz de Flujos de Tráfico Permitidos

Para aplicar una política de *Zero Trust* a nivel de red, se sustituye el modelo de "permitir todo excepto lo prohibido" por una estrategia de **"Deny All" (Denegar todo por defecto)**. Solo se permiten explícitamente los siguientes flujos documentados:

Origen (Zona)	Destino (Zona)	Protocolo / Puerto	Justificación Operativa
Red Corp (Nivel 4)	IDMZ (Nivel 3.5)	HTTPS (443), RDP (3389)	Acceso de usuarios IT autorizados a los Servidores de Salto (Jump Hosts) y consulta de informes en el Historian Espejo.
IDMZ (Nivel 3.5)	Red OT (Nivel 3)	S7Comm, Modbus (502)	Replicación unidireccional de datos desde el SCADA principal hacia el Espejo en la DMZ.
IDMZ (Nivel 3.5)	Red OT (Nivel 3)	SMB (445)	Distribución de parches de seguridad desde el servidor WSUS centralizado (solo durante ventanas de mantenimiento).
Red OT (Nivel 3)	Red Control (Nivel 1)	Modbus/TCP (502)	Envío de comandos de operación y lectura de telemetría desde la Sala de Control hacia los PLCs.
CUALQUIERA (Niveles 0-3)	INTERNET	BLOQUEADO	Los niveles 0, 1, 2 y 3 tienen prohibida técnica y físicamente la salida directa a Internet.

12. PLAN DE RESPUESTA ANTE INCIDENTES Y RECUPERACIÓN (PRI)

12.1 Marco de Actuación (Ciclo de Vida del Incidente)

El Plan de Respuesta ante Incidentes (PRI) de Alpha-V se adhiere metodológicamente a la guía **NIST SP 800-61 Rev. 2** (Computer Security Incident Handling Guide). Este marco garantiza que la respuesta no sea improvisada, sino que siga un flujo de trabajo cíclico y auditado.

El objetivo prioritario ante cualquier incidente en la central es, invariablemente, **garantizar la seguridad física (*Safety*)** del reactor y de las personas, subordinado la preservación de los activos IT a esta premisa superior.

12.2 Playbook Específico: [PB-01] Ransomware en Entorno OT

Dada la criticidad del riesgo de secuestro de sistemas industriales (ej. *LockerGoga*, *Ekans*), se establece el siguiente protocolo de actuación paso a paso.

PLAN DE RESPUESTA A INCIDENTES DE CIBERSEGURIDAD: RANSOMWARE CRÍTICO (Modelo OT-IT)

Este plan detalla los pasos a seguir ante un incidente de ciberseguridad clasificado como Crítico, con foco en el riesgo de propagación de un ataque de *ransomware* desde la red corporativa (IT) hacia la red de control industrial (OT)

FASE 1: DETECCIÓN Y ANÁLISIS PRELIMINAR (Triaje y Verificación)

El objetivo inicial es confirmar la naturaleza del ataque y su severidad para movilizar los recursos adecuados.

- **Vector de Alerta Crítico:** La alarma se dispara al detectarse indicadores de compromiso (IoCs) de alta fidelidad, que no dejan lugar a dudas sobre un ataque activo:
    1. **SIEM (*Security Information and Event Management*): Splunk** (o herramienta equivalente) genera una alerta de correlación por volumen inusual de actividad.
        - **Criterio 1:** Detección de un **cifrado masivo y simultáneo** de archivos sensibles o históricos en el **Servidor Historian** (Nivel 3.5/4) o en cualquier Servidor de Producción IT.
        - **Criterio 2:** Comunicaciones salientes persistentes e inusuales hacia direcciones IP conocidas como **infraestructura de *Command & Control* (C2)** de grupos de *ransomware* conocidos, saltando los filtros del *proxy*.
- **Acción Inmediata del Centro de Operaciones de Seguridad (SOC L1/L2):**
    1. **Validación de la Alerta (Falso Positivo):** Se realiza una revisión rápida de los *logs* y la telemetría del EDR (Endpoint Detection and Response) para confirmar que la actividad maliciosa es real y no una actualización de software o un proceso legítimo erróneo.
    2. **Clasificación de la Severidad:** Dada la afectación de servidores críticos (Historian) o la presencia de C2, la clasificación es **CRÍTICA (Nivel 1)**. El riesgo de pérdida de datos, parada de producción y daño reputacional es máximo.
    3. **Movilización de Equipos:** Se activa de forma inmediata el **Comité de Crisis** (CISO, CIO, Director de Operaciones, Asesor Legal) y se notifica sin demora al **CSIRT** (Equipo de Respuesta a Incidentes de Ciberseguridad) y al **CISO** (Chief Information Security Officer) para la toma de decisiones estratégicas.

FASE 2: CONTENCIÓN Y MITIGACIÓN DE DAÑOS ("Detener la Hemorragia")

La prioridad absoluta es evitar la propagación lateral del *ransomware*, especialmente el salto de la red IT a la red OT y la potencial interrupción de los procesos de la planta.

- **Aislamiento de Red (Segmentación y Contención):**
  - **Paso 1: Ejecución del "Corte de lDMZ" (DMZ Industrial).** Esta es la acción más crítica. El equipo de Redes y el CSIRT deben aplicar una regla de **Denegar Todo (Drop/Reject)** en el *Firewall Palo Alto* (o equivalente) que gestione el tráfico entre la Zona IT (Nivel 3.5/4) y la Zona de Control Industrial (Nivel 3).
    - **Resultado Esperado:** La planta de OT queda **aislada digitalmente** de la red corporativa, operando en **modo "Isla"**. Los procesos de control (PLCs, HMIs) continúan activos, pero cualquier comunicación desde/hacia IT queda bloqueada.
  - **Paso 2: Principio Forense (No Apagar). Bajo ninguna circunstancia se deben apagar** los equipos, servidores o estaciones de trabajo que se identifiquen como infectados.
    - **Justificación:** Apagar un sistema operativo elimina la evidencia volátil crucial residente en la memoria RAM (claves de cifrado generadas por el *ransomware*, procesos inyectados, comunicación de *sockets*).
  - **Paso 3: Desconexión Física y Lógica.** Para detener la propagación lateral (ej. a través de SMB o RDP) mientras se mantiene la memoria activa, se debe:
    - **Desconectar el cable de red físico (RJ-45)** de los activos comprometidos.
    - **Bloquear el puerto en el switch** de la red afectada (Shutdown Port).
    - Aplicar una **regla de *firewall* local** a los activos infectados que impida toda comunicación saliente.

FASE 3: ADQUISICIÓN FORENSE DIGITAL (Preservación de Evidencia)

Antes de cualquier intento de erradicación o limpieza, es imperativo asegurar la cadena de custodia y recolectar la evidencia volátil y persistente.

- **Adquisición de Memoria Volátil (RAM *Dumping*):**
    - **Metodología:** El equipo forense utiliza herramientas de respuesta en vivo (*Live Response*) como **FTK Imager** o **Velociraptor** cargadas en un pendrive USB previamente analizado y seguro.
    - **Objetivo Primario:** Volcar una imagen completa de la RAM. Se prioriza la búsqueda de la **clave de descifrado** del *ransomware* (que a menudo reside en memoria antes de ser borrada) o la identificación binaria exacta del *malware* para generar firmas de detección.
- **Clonado de Disco (Imagen Forense Bit a Bit):**
    - **Extracción y Bloqueo:** Se extraen físicamente los discos duros (SSD/HDD) de los servidores críticos afectados. Estos se conectan obligatoriamente a **Bloqueadores de Escritura (*Tableau Write Blockers*)** para garantizar que ningún dato sea modificado.
    - **Generación de Imagen:** Se crea una imagen forense **bit a bit** de los discos originales, generalmente en formato E01.
    - **Validación de Evidencia:** Se calcula y documenta el **Hash Criptográfico (SHA-256)** de la imagen forense. Esta imagen es la única que se analiza; el disco duro original es **precintado** con documentación de la cadena de custodia y depositado en la caja fuerte de evidencias.

FASE 4: ERRADICACIÓN Y RECUPERACIÓN (*Clean Room* y Hardening)

Esta fase se centra en eliminar la amenaza y restaurar los sistemas de forma segura, garantizando la no recurrencia.

- **Limpieza de la Infraestructura:**
    1. **Identificación y Eliminación del Vector de Entrada:** Análisis forense para determinar el punto de origen del compromiso (ej. un servidor de borde vulnerable, una cuenta **VPN comprometida** debido a un factor de autenticación débil, un correo de *phishing* exitoso, o una vulnerabilidad **sin parchear** en un sistema crítico). El vector debe ser cerrado antes de restaurar.
- **Restauración Segura de Datos (Protocolo 3-2-1-1-0 Reforzado):** Se utiliza una metodología estricta para garantizar que el *ransomware* no esté latente en los backups.
    1. **Acceso al Backup Inmutable:** Se accede exclusivamente al **Repositorio de Backup de Retención Larga e Inmutable** (idealmente un sistema Linux Hardened o *Air-Gapped* como el definido en la Iniciativa de Resiliencia 4).
    2. **Entorno de Cuarto Limpio (*Sandbox*):** Los datos y las imágenes del sistema se restauran **primero** en un entorno totalmente **aislado y virtual** de "Cuarto Limpio" (*Clean Room*). Este ambiente simula la producción sin tener conectividad de red real.
    3. **Doble Escaneo de Seguridad:** La copia restaurada se somete a un escaneo exhaustivo utilizando **dos motores antivirus/EDR distintos** y avanzados. El objetivo es identificar cualquier "bomba de tiempo" latente (*sleeper* malware) que pueda reactivarse post-restauración.
    4. **Despliegue a Producción:** Solo una vez que la copia ha sido validada y declarada limpia, la imagen del sistema operativo y los datos se vuelcan a los nuevos servidores o a los servidores de Producción previamente formateados y endurecidos (*re-imaged*).

FASE 5: LECCIONES APRENDIDAS Y POST-MORTEM (Resiliencia Operativa)

La fase final busca la mejora continua del estado de seguridad de la organización.

- **Informe Ejecutivo del CISO:** En un plazo máximo de **72 horas** tras la declaración de cierre del incidente, el CISO debe presentar un informe detallado a la dirección y al Comité de Crisis que contenga:
    - **Cronología Detallada (Timeline):** Reconstrucción exacta, minuto a minuto, del ataque (detección, contención, acciones tomadas).
    - **Impacto Financiero y Operacional:** Cálculo del **coste estimado del impacto** (coste directo por *hardware* y consultoría, coste indirecto por parada de producción, horas hombre del personal interno, posibles multas regulatorias).
    - **Propuesta de Mejoras Técnicas (*Hardening*):** Un plan de acción con partidas presupuestarias específicas para **evitar la recurrencia**. Ejemplos:
        - Ajustar reglas de correlación del SIEM para reducir el tiempo de detección.
        - Implementar MFA (Autenticación Multifactor) obligatorio en todas las cuentas VPN y críticas.
        - Endurecer políticas de contraseñas y reducir privilegios.
        - Inversión en soluciones de Micropsegmentación en la red OT.

---

13. CONCLUSIONES Y RECOMENDACIONES FINALES

El presente Plan Director de Seguridad "NuclearShield" ha sido diseñado para abordar uno de los desafíos más complejos de la ingeniería actual: la protección de infraestructuras críticas en un escenario de ciberamenazas asimétricas y persistentes. Tras el análisis de riesgos, la definición de la arquitectura y la planificación de la respuesta, se extraen las siguientes conclusiones estratégicas:

1. **Cumplimiento Normativo como Motor de Cambio:** La alineación con el **Esquema Nacional de Seguridad (ENS) en su Categoría Alta** y la Ley 8/2011 de Protección de Infraestructuras Críticas no se ha abordado como un mero trámite burocrático, sino como la base para estructurar una defensa robusta. El proyecto garantiza que Alpha-V no solo cumple con la legalidad vigente, evitando sanciones, sino que eleva su estándar de operación al nivel exigido por la seguridad nacional.
2. **Convergencia IT/OT Segura:** Se ha superado el mito de la "seguridad por oscuridad" o el aislamiento total (Air-Gap), que en la Industria 4.0 es impracticable. Mediante la implementación del **Modelo Purdue Reforzado**, la creación de la IDMZ y el uso de **Diodos de Datos**, se ha logrado habilitar la digitalización del negocio (monitorización en tiempo real) sin comprometer la seguridad física (*Safety*) del reactor.
3. **Cambio de Paradigma: De la Prevención a la Resiliencia Forense:** Asumiendo que "la intrusión es inevitable", el plan ha priorizado la capacidad de detección y respuesta (*Forensic Readiness*). La inversión en un SOC híbrido, sistemas SIEM y almacenamiento de logs inmutables (WORM) dota a la organización de la capacidad legal y técnica para investigar incidentes, atribuir responsabilidades y recuperarse de ataques destructivos como el Ransomware.
4. **Viabilidad y Retorno de la Inversión (ROI):** Si bien la implementación del plan requiere una inversión inicial significativa en tecnología (NGFW, PAM, SIEM) y capital humano, el coste es infinitesimal comparado con el impacto económico, reputacional y social de una parada no programada del reactor o un incidente radiológico provocado por un ciberataque.

Recomendación Final: Se recomienda a la Dirección de Alpha-V la aprobación inmediata de la **Iniciativa 1 (SOC)** y la **Iniciativa 4 (Backup Inmutable)** como prioridades de ejecución en el primer trimestre (Q1). La ventana de exposición actual es inaceptable, y estas medidas reducirán el riesgo inherente en un 60% en los primeros 90 días de proyecto.

---

14. REFERENCIAS BIBLIOGRÁFICAS Y NORMATIVA

Para la elaboración del presente Plan Director de Seguridad se han consultado, analizado y aplicado los siguientes cuerpos normativos, estándares internacionales y guías de buenas prácticas:

14.1 Legislación y Regulación Nacional (España)

El marco jurídico de cumplimiento obligatorio que vertebra este proyecto:

- **Ley 8/2011**, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (Ley PIC).
- **Real Decreto 704/2011**, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- **Real Decreto 311/2022**, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- **Instrucción IS-30 (Revisión 2)**, del Consejo de Seguridad Nuclear (CSN), sobre requisitos de seguridad física en las instalaciones nucleares y de transporte de materiales nucleares.
- **Resolución de 13 de octubre de 2016**, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad.

14.2 Estándares Internacionales de Ingeniería y Seguridad

Referentes técnicos para la arquitectura de redes y gestión de riesgos:

- **IEC 62443 (Industrial Automation and Control Systems Security):**
  - *Part 3-2:* Security Risk Assessment for System Design.
  - *Part 3-3:* System Security Requirements and Security Levels.
- **NIST Special Publications (National Institute of Standards and Technology):**
  - *NIST SP 800-82 Rev. 2:* Guide to Industrial Control Systems (ICS) Security.
  - *NIST SP 800-61 Rev. 2:* Computer Security Incident Handling Guide.
  - *NIST SP 800-53 Rev. 5:* Security and Privacy Controls for Information Systems.
- **ISO/IEC 27000 Series:**
  - *ISO/IEC 27001:2022:* Sistemas de Gestión de la Seguridad de la Información (Requisitos).
  - *ISO/IEC 27035:* Gestión de incidentes de seguridad de la información.
  - *ISO 22301:2019:* Sistemas de gestión de la continuidad del negocio (BCMS).

14.3 Guías Técnicas del Centro Criptológico Nacional (CCN-STIC)

Documentación técnica de referencia para la adecuación al ENS:

- **CCN-STIC-800:** Guía de Adecuación al Esquema Nacional de Seguridad.
- **CCN-STIC-401:** Glosario de Términos y Abreviaturas de Ciberseguridad.
- **CCN-STIC-480:** Ciberseguridad en Sistemas de Control Industrial.
- **CCN-STIC-883:** Guía de Implementación de SIEM en el ENS.

14.4 Metodologías y Marcos de Trabajo

- **MAGERIT v.3:** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Libro I: Método y Libro II: Catálogo de Elementos).
- **MITRE ATT&CK for ICS:** Base de conocimiento de tácticas y técnicas de adversarios en entornos industriales.
- **Modelo Purdue (PERA):** Purdue Enterprise Reference Architecture para la segmentación de redes CIM/CI.

ANEXO A: DECLARACIÓN DE USO DE INTELIGENCIA ARTIFICIAL

A.1 Declaración de Conformidad y Metodología De conformidad con los criterios de evaluación establecidos para el Trabajo de Fin de Grado y en aras de la transparencia académica, se declara explícitamente el uso de herramientas de Inteligencia Artificial como soporte auxiliar durante el desarrollo del proyecto "NuclearShield".

El uso de estas herramientas se ha regido estrictamente por el principio de **"Human-in-the-Loop" (Supervisión Humana)**, limitándose a las siguientes funciones:

1. **Estructuración y Ideación:** Apoyo en la definición del índice y la organización lógica de los contenidos (Modelo en V, fases de implementación).
2. **Generación de Activos Sintéticos:** Creación de escenarios de riesgo hipotéticos y datos simulados para las matrices de evaluación (dado que no se dispone de datos reales de una central nuclear por motivos de confidencialidad).
3. **Soporte de Redacción Técnica:** Asistencia en la redacción de descripciones técnicas de protocolos estándar (Modbus, IEC 62443) y revisión de estilo para mantener un tono formal y consultivo.
4. **Generación de Elementos Visuales:** Creación de imágenes conceptuales para portadas y diagramas mediante DALL-E 3 / Midjourney.

A.2 Responsabilidad de Contenidos El autor del presente proyecto certifica que **todos los resultados generados por la IA han sido revisados, validados y corregidos manualmente**. La veracidad técnica, los cálculos de riesgo y las decisiones estratégicas son responsabilidad exclusiva del alumno, habiéndose contrastado la información con las fuentes bibliográficas oficiales citadas (CCN-CERT, NIST, BOE).

A.3 Registro de Prompts (Ingeniería de Instrucciones) A continuación, se documentan los principales *prompts* (instrucciones) utilizados para la elaboración de los distintos bloques del proyecto, demostrando la metodología de trabajo empleada:

Fase del Proyecto	Herramienta	Prompt (Instrucción) Utilizada
Contexto y Normativa	Gemini Advanced	"Actúa como un experto en cumplimiento normativo (GRC). Genera una tabla comparativa entre el marco NIST SP 800-82, la ISO 27001 y el Esquema Nacional de Seguridad (ENS), destacando las ventajas de cada uno para una infraestructura crítica nuclear."
Análisis de Riesgos	ChatGPT-4	"Basándote en la metodología MAGERIT v.3, ayúdame a identificar 5 amenazas específicas para entornos OT (Tecnología de Operación). Para cada amenaza (ej. Ransomware, Sabotaje), propón una valoración de Impacto y Probabilidad justificada en un entorno de alta seguridad."
Iniciativas Técnicas	Gemini Advanced	"Redacta una ficha técnica detallada para una iniciativa de segmentación de redes industriales basada en el Modelo Purdue. Debe incluir conceptos como zona IDMZ, servidores de salto (Jump Hosts) y el uso de Diodos de Datos para garantizar la unidireccionalidad hacia el nivel de gestión."
Arquitectura de Red	Gemini Advanced	"Desarrolla una matriz de flujos de tráfico para un Firewall NGFW que proteja una red SCADA. Define reglas de 'Deny All' y especifica qué puertos y protocolos (Modbus TCP/502, S7Comm) deben permitirse estrictamente entre la zona de Supervisión y la zona de Control."
Respuesta a Incidentes	ChatGPT-4	"Crea un Playbook de respuesta ante incidentes paso a paso siguiendo la guía NIST SP 800-61 para un escenario de infección por Ransomware en un servidor Historian. Incluye fases de: Detección, Contención (aislamiento de red), Erradicación y Recuperación (Backup inmutable)."

Fase del Proyecto	Herramienta	Prompt (Instrucción) Utilizada
Elementos Visuales	DALL-E 3	"Genera una imagen fotorrealista y profesional para la portada de un proyecto de ciberseguridad nuclear. Debe mostrar un escudo digital abstracto en tonos azul marino protegiendo una torre de refrigeración, con estilo tecnológico y minimalista."