



CERTIFICACIÓN

INFORME DE AUDITORÍA: TRIPODE PARTNERS GROUP, S.L.

TIPO DE VISITA:

**AUDITORÍA DE SEGUIMIENTO 3.3 (ENAC -
ISO/IEC 27001:2022)**

NÚMERO DE CONTRATO:

ES/BAL/2017002233

BE THE BENCHMARK

SGS

SGS Oficina Proveedora:	SGS INTERNATIONAL CERTIFICATION SERVICES IBÉRICA, S.A. (Unipersonal)	
Organización (Cliente):	TRIPODE PARTNERS GROUP, S.L.	
Dirección (Oficina Central):	Galileo Galilei, 2, Edificio U, Planta baja, Local 1, 07121, PARC BIT, Palma de Mallorca, Baleares España	
Zastopnikpersona De Contacto En El Cliente:	Marta Montserrat	
CRITERIOS DE AUDITORÍA		
Acreditación	Oficina SGS Acreditada	Número efectivo de empleados
ENAC	SGS INTERNATIONAL CERTIFICATION SERVICES IBÉRICA, S.A. (Unipersonal)	3
Norma / Esquema	Alcance De Certificación	
ISO/IEC 27001:2022	El Sistema de Información que soportan los procesos de negocio siguientes: Distribución de producto turístico, empresa a empresa (B2B) y empresa a cliente (B2C) Según declaración de aplicabilidad V1.	

Asignación del Equipo Auditor	
Auditor jefe	Antonio MAMPEL MATEU - Auditor
Otros Acompañantes (Nombre Y Función)	
Fecha(s) De Auditoría	26 feb. 2026

1. OBJETIVOS DE AUDITORÍA

Los objetivos de esta auditoría/visita son, para el alcance de la certificación:

Determinar la conformidad del sistema de gestión del cliente, o partes de éste, con los criterios de auditoría;

Determinar la capacidad del sistema de gestión para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables (NOTA: una auditoría de certificación de un sistema de gestión no es una auditoría de cumplimiento legal);

Determinar la eficacia del sistema de gestión para alcanzar, de un modo razonable, sus objetivos;

Si procede, la identificación de posibles áreas de mejora del sistema de gestión.

CONSIDERACIONES:

El alcance de la auditoría, así como las fechas y lugares donde ésta se ha realizado se identifican en el plan de auditoría (cualquier cambio se identifica en el informe de auditoría).

Este informe de auditoría contiene un resumen de la capacidad del sistema de gestión para cumplir los requisitos aplicables y los resultados esperados.

Este informe es confidencial y su distribución se limita al equipo auditor, asistentes a la auditoría, representante del cliente, oficina de SGS y, si aplica, entidad de acreditación, propietarios del esquema y cualquier otra entidad reglamentaria, en línea con nuestra Política de Privacidad accesible en www.sgs.es/es-es/privacy-at-sgs.

Las auditorías se realizan mediante un proceso de muestreo, con base en la información disponible en el momento de la auditoría. Los métodos de auditoría deben incluir, pero no limitarse a: entrevistas, observación de las actividades y revisión de documentos y registros.

2. RESUMEN Y CONCLUSIONES

CONCLUSIONES

El equipo auditor recomienda, con base en los resultados de esta auditoría, que la certificación para el sistema de gestión sea:

NORMA Y ACREDITACIÓN	CONCLUSIONES
ISO/IEC 27001:2022 - ENAC	Mantenida

La continuidad de la certificación está condicionada al tratamiento adecuado de las no conformidades.

RESUMEN DE LA AUDITORIA

- La documentación del sistema de gestión ha demostrado su conformidad con los requisitos de la(s) norma(s) de auditoría y proporciona la estructura suficiente para respaldar la implementación y el mantenimiento del sistema de gestión.
- La organización ha demostrado una implementación y un seguimiento eficaces de la capacidad de su sistema de gestión en relación con el cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables.
- A lo largo del proceso de auditoría, el sistema de gestión demostró conformidad general con los requisitos de la(s) norma(s) de auditoría.

Número de no conformidades identificadas	0
--	---

- El alcance de la certificación es adecuado.
- Se han cumplido los objetivos de la auditoría
- Se ha seguido el plan de auditoría.
- El programa de auditoría es adecuado.
- Se ha resuelto cualquier cuestión.

3. HALLAZGOS DE LA AUDITORIA PREVIA

Se han revisado los resultados de la última auditoría, en particular para asegurar la implantación de acciones correctoras adecuadas en el caso de haberse identificado no conformidades (o hallazgos en la Etapa 1). Cuando el sistema de gestión no hubiera realizado un tratamiento adecuado, el problema concreto se habrá identificado como no conformidad en este informe.

4. NO CONFORMIDADES

n/a

5. OBSERVACIONES Y OPORTUNIDADES DE MEJORA

Observación Nº 1	
Descripción	Contemplado en los aspectos del cambio climático se nota faltar alguna de las especificaciones indicadas por la Comisión del Del cambio climático establecida en la Unión Europea.
Norma / Esquema	ISO/IEC 27001:2022
Proceso	SUR3P ESTATEGICOS Y PLANIFICACIÓN
Elementos obligatorios:	

Observación Nº 2	
Descripción	No se ha especificado La traza De manera adecuada entre los tratamientos y los objetivos de seguridad de la información, Se intuyen Pero no se puede evidenciar.
Norma / Esquema	ISO/IEC 27001:2022
Proceso	SUR3P ESTATEGICOS Y PLANIFICACIÓN
Elementos obligatorios:	

Observación Nº 3	
Descripción	Repercutir los niveles competenciales en todos los sistemas de gestión de la organización.
Norma / Esquema	ISO/IEC 27001:2022
Proceso	SUR3P SOPORTE
Elementos obligatorios:	

Observación Nº 4	
Descripción	Los controles con los tres requisitos (negocio, contractual y legal) deben priorizarse en la hoja de ruta, ya que el incumplimiento genera riesgos simultáneos en operaciones, relaciones comerciales y cumplimiento normativo
Norma / Esquema	ISO/IEC 27001:2022
Proceso	SUR3 OPERACIONES
Elementos obligatorios:	

6. REQUISITOS ESPECÍFICOS

¿Cambios significativos?

No

7. LINEAS DE INVESTIGACIÓN DE AUDITORIA

SITIO 1: TRIPODE PARTNERS GROUP, S.L. - Galileo Galilei, 2, Edificio U, Planta baja, Local 1, 07121, PARC BIT, Palma de Mallorca, Baleares España

Proceso: SUR3P ESTATEGICOS Y PLANIFICACIÓN

Propietario Del Proceso	Auditor(a)
Comité SGSI	Antonio MAMPEL MATEU
Resumen	
<p>.Contexto, Partes interesadas, Alcance, requisitos del sistema. Liderazgo, Política, Roles, responsabilidades y autoridad</p> <p>Plan Estratégico 2025–2027 “Brand's Challenge” y Cambio Cultural</p> <p>El anterior Plan Estratégico “MindSet Digital” se ha creado marca reconocida en el mercado.</p> <p>ahora posicionarnos en torno al cliente que se quiere y a cuales se puede llegar con los desarrollos realizados</p> <p>cambio cultural, en la organización, cambios nuevos equipos de trabajo y formas de trabajar. Sera dirigido por el consejo de administración y ejecutado por la directora general y los responsables jefes de área, visión estratégica holística. Compromiso de filosofía de empresa como actuar misión visión y valores revisados y transmitidos a todo el personal.</p> <p>OBS: Contemplado en los aspectos del cambio climático se nota faltar alguna de las especificaciones indicadas por la Comisión del Del cambio climático establecida en la Unión Europea.</p> <p>Se matiene el alcance</p> <p>Partes interesadas se mantiene la estructura, Necesidades expectativas y requisitos de cada una de ellas Asimismo se contempla los procesos en los que se ve involucrada la parte interesada. La retroalimentación de dichas partes para la mejora continua.</p> <p>Mapa de procesos, Se establece un mapa de procesos Que contempla Procesos estratégicos procesos operativos Y de apoyo Cada 1 de ellos Indica los procedimientos o procesos Relacionados.</p> <p>Dentro de los procesos estratégicos se contemplan Las políticas como la mejora continua como el análisis de riesgos como la gestión del talento com Investigación desarr E innovación. Se establece el responsable de cada 1 de los procesos .</p> <p>Como procesos operativos Destacan los de gestión de infraestructuras de IT Diseño y desarrollo del servicio y la gestión y gobernanza del dato . Dentro de los procesos de apoyo se diferencian los financieros, Procesos relacionados con El grc , ventas y comunicación y marketing.</p> <p>Los subprocesos Vienen descritos los procedimientos el personal que interviene el equipo de trabajo los riesgos y los seguimientos que se llevan a cabo Enlazándolo con Los proyectos personal O actividad a realizar En dicho proceso.</p> <p>Lderazgo: Establecido el plan estratégico se indican Las actuaciones Y metas a conseguir En el proceso de implantación Del Brand’s Challenge.</p>	

También se contemplan la revisión por la dirección y el seguimiento de la documentación Así Los nuevos cambios implementados en cada una de las áreas.

Roles y responsabilidades, mapa funcional en función de los objetivos estratégicos, tb existen DPT para cada uno de los puestos de trabajo donde se especifican los niveles competenciales para cada uno de los sistemas de gestión.

Sede la descripción De cada 1 De los puestos con relevancia De la empresa tecnológica CEO CIO CTO CFO, ETC. Así como la dependencia jerárquica con cada 1 de los especialistas necesarios en las distintas áreas.

PLANIFICACIÓN, Enfoque a riesgos y tratamiento, Objetivos y gestión del cambio.

Se enfoca el análisis de riesgos teniendo en cuenta los procesos y los activos de información relacionados con los mismos A partir de aquí se determinan Las vulnerabilidades y amenazas que se puedan manifestar en cada 1 de ellos. Teniendo en cuenta el impacto la probabilidad la detectabilidad se calcula el riesgo y se establece el responsable del riesgo.

Entre otros riesgos Se detectan:

La existencia de riesgo de ataque por denegación de servicio ODOS Para explotar las debilidades de una configuración débil en la infraestructura.

El riesgo de un ataque de phishing explotando la falta de formación del personal y comprometiendo credenciales y acceso a los sistemas críticos.

Riesgo de cifrado malicioso en los sistemas críticos por vulnerabilidades técnicas no corregidas.

Así hasta un total de 24 riesgos Analizados, Sean considerados los más importantes o relevantes para la consecución de los objetivos estratégicos de la organización.

Se establece la acción a realizar en cada 1 de los riesgos mitigar , transferir o eliminar el riesgo.

De dichas acciones se desprenden tareas Detalladas, A modo de evidencia migración del SQL Server Cuyo objetivo es mejorar el performance , mantener una estructura actualizada y alineada con las mejores prácticas , EY reducir la implicación en la gestión del sistema operativo. Establecidas las subtareas y actividades vinculadas, Se tienen en cuenta La necesidad de recursos para poderlas llevar a cabo tanto en personas como hora Compra de elementos necesarios Para su solución. Se establece un historial Del tratamiento y de las acciones así como una medición de las mismas Para la consecución De los mismos.

De igual forma se tratan Las oportunidades detectadas durante el análisis de riesgo y el procesamiento De las actividades.

OBS: No se ha especificado La traza De manera adecuada entre los tratamientos y los objetivos de seguridad de la información, Se intuyen Pero no se puede evidenciar.

Objetivo1: Mejorar la postura de seguridad de la información desde la organización. Formación, Vigilancia activa del sistema, indicadores y controles asociados.

A.5.6 A27002-150 - A.5.6 Contacto con grupos de interés especial REVISADO Sí Requisito de negocio DOC-SGSI Contacto con las autoridades, Este control establece que la organización debe mantener relaciones proactivas con autoridades competentes (como fuerzas de seguridad, reguladores de ciberseguridad o agencias de protección de datos) y otros grupos especializados. El objetivo es facilitar el intercambio de información sobre amenazas, obtener asesoramiento técnico y asegurar una respuesta coordinada ante incidentes graves o requerimientos legales. No se trata solo de llamar a la policía cuando hay un robo, sino de tener canales establecidos para reportar ciberataques complejos o consultar normativas específicas.

A.5.7 A27002-151 - A.5.7 Inteligencia de amenazas Tareas por hacer Sí Requisito de negocio Requisito contractual PS-SGSI Inteligencia de amenazas. Implica la implementación de procesos para recopilar, analizar y utilizar información sobre amenazas de seguridad actuales y emergentes. La organización debe monitorear fuentes externas (informes de seguridad, feeds de inteligencia, comunidades técnicas) para entender qué actores están atacando, qué vulnerabilidades están siendo explotadas y cómo adaptar sus defensas antes de ser víctima. Es pasar de una postura reactiva a una

preventiva basada en datos reales del panorama de amenazas.

A.5.27 A27002-171 - A.5.27 Aprendizaje de los incidentes de seguridad de la información En curso Sí Requisito de negocio Requisito contractual. Tras gestionar un incidente, este control exige realizar un análisis post-mortem para extraer lecciones aprendidas. No basta con resolver el problema; la organización debe documentar qué funcionó, qué falló y cómo mejorar los procesos, herramientas o capacitación para evitar que el mismo incidente se repita o para mitigar su impacto en el futuro. Es el ciclo de mejora continua aplicado a la seguridad.

A.5.28 A27002-172 - A.5.28 Recolección de evidencias En curso Sí Requisito de negocio. Define los procedimientos para identificar, recolectar, almacenar y proteger la evidencia digital necesaria para investigaciones internas o procesos legales. Esto es crítico para garantizar que la evidencia sea admisible en un tribunal (cadena de custodia intacta) y para realizar análisis forenses precisos sin alterar los datos originales. Incluye el uso de herramientas adecuadas y protocolos estrictos de manejo de datos.

A.5.31

A27002-175 - A.5.31 Requisitos legales, estatutarios, regulatorios y contractuales Tareas por hacer. Sí Requisito de negocio Requisito contractual Requisito legal. La organización debe identificar, documentar y mantenerse al día con todas las leyes, regulaciones y obligaciones contractuales aplicables a la seguridad de la información. Esto abarca desde leyes de protección de datos (como GDPR o leyes locales), regulaciones sectoriales específicas hasta cláusulas de confidencialidad con clientes. El objetivo es asegurar el cumplimiento normativo continuo y evitar sanciones legales o multas.

A.6.7 A27002-188 - A.6.7 Trabajo remoto En curso Sí Requisito de negocio. Trabajo remoto Establece directrices para asegurar la seguridad de la información cuando los empleados trabajan fuera de las instalaciones de la organización (teletrabajo, movilidad). Esto incluye la protección de dispositivos personales o corporativos usados remotamente, el uso de conexiones seguras (como VPNs), la gestión de accesos remotos y la concienciación sobre riesgos específicos del entorno doméstico o público (pantallas visibles, redes Wi-Fi inseguras).

A.8.14 A27002-217 - A.8.14 Redundancia de las instalaciones de procesamiento de información En curso Sí Requisito de negocio, Busca garantizar la disponibilidad de los sistemas críticos mediante la implementación de infraestructura redundante. Si un centro de datos, servidor o enlace de red falla, existe un componente o sitio alternativo listo para tomar el relevo inmediatamente o en un tiempo muy corto. Esto es fundamental para cumplir con los objetivos de recuperación ante desastres y asegurar la continuidad del negocio frente a fallos técnicos o catástrofes.

A.8.24 A27002-227 - A.8.24 Uso de criptografía En curso Sí Requisito de negocio Requisito contractual Requisito legal. NS-SGSI-Norma de controles criptográficos PS-SGSI-Gestión Claves Seguras. Define las políticas y procedimientos para el uso correcto de técnicas criptográficas (cifrado, firmas digitales, certificados) para proteger la confidencialidad, integridad y autenticidad de la información. Este control no solo exige usar cifrado, sino hacerlo de manera estandarizada, gestionando correctamente el ciclo de vida de las claves criptográficas (generación, almacenamiento, rotación y destrucción) para evitar que la protección sea ineficaz o vulnerable.

Proceso: SUR3 OPERACIONES

Propietario Del Proceso	Auditor(a)
Comité SGSI	Antonio MAMPEL MATEU
Resumen	
Establecido el soporte de información y su seguridad para los procesos de distribución de producto turístico, empresa a empresa (B2B) y empresa a	

cliente (B2C) y la realización de estas actividades su contexto y partes interesadas se analizan en los riesgos identificados para la consecución de los objetivos. De los tratamientos y controles establecidos y mapeados con el Anexo A se describen entre otros, los siguientes controles relacionados con los procesos en los que se tienen en cuenta.

A.5.20 A27002-164 - A.5.20 Requisitos de seguridad de la información en contratos con terceros En curso Sí Requisito de negocio Requisito contractual
Requisito legal: | Negocio + Contractual + Legal Este control exige que todos los acuerdos con proveedores incluyan cláusulas específicas de seguridad de la información. Desde el negocio, protege los activos que comparten terceros. Contractualmente, asegura que los proveedores cumplan con los mismos estándares que la organización. Legalmente, algunas regulaciones (como GDPR) exigen responsabilidad compartida sobre datos procesados por terceros. La implementación requiere revisar y actualizar todos los contratos vigentes.

A.5.21 A27002-165 - A.5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC Tareas por hacer Sí Requisito de negocio |
Requisito de negocio Se enfoca en evaluar y monitorear la seguridad de proveedores de tecnología críticos. Como requisito de negocio, evita que vulnerabilidades en la cadena de suministro afecten operaciones propias. No suele tener mandato legal directo, pero es esencial para la continuidad operativa. Implica clasificar proveedores por criticidad y establecer niveles de verificación según el riesgo que representan.

A.8.3 A27002-206 - A.8.3 Restricción de acceso a la información REVISADO Sí Requisito de negocio Requisito contractual Requisito legal | Negocio +
Contractual + Legal Principio de mínimo privilegio aplicado a toda la información. Negocio: protege activos sensibles internos. Contractual: clientes exigen garantías de que solo personal autorizado accede a sus datos. Legal: leyes de protección de datos obligan a limitar accesos a información personal. Requiere políticas de clasificación de información y revisiones periódicas de permisos.

A.8.4 A27002-207 - A.8.4 Acceso al código fuente En curso Sí Requisito de negocio Requisito contractual Requisito legal | Negocio + Contractual + Legal
Controla quién puede acceder al código fuente de sistemas críticos. Negocio: protege propiedad intelectual y secretos comerciales. Contractual: algunos clientes requieren auditorías de código como condición de contratación. Legal: ciertas industrias (banca, salud) tienen regulaciones sobre trazabilidad de cambios. Debe incluir registros de acceso y justificación documentada.

A.8.5 A27002-208 - A.8.5 Autenticación segura En curso Sí Requisito de negocio Requisito contractual Requisito legal | Negocio + Contractual + Legal
Implementa mecanismos robustos de verificación de identidad. Negocio: previene accesos no autorizados a sistemas internos. Contractual: SLAs con clientes suelen exigir MFA o estándares específicos. Legal: regulaciones sectoriales pueden requerir autenticación fuerte para ciertos datos. Incluye gestión de contraseñas, MFA y revocación de credenciales.

A.8.8 A27002-211 - A.8.8 Gestión de las vulnerabilidades técnicas En curso Sí Requisito de negocio Requisito contractual Requisito legal NS-SGSI Gestión
Operaciones PS-SGSI-Corrección de Vulnerabilidades Técnicas. | Negocio + Contractual + Legal Proceso sistemático para identificar y corregir vulnerabilidades. Negocio: reduce riesgo de incidentes operativos. Contractual: clientes exigen parcheo dentro de plazos definidos. Legal: algunas regulaciones establecen tiempos máximos de corrección. Requiere inventario de activos, escaneo regular y proceso de remediación documentado

A.8.17 A27002-220 - A.8.17 Sincronización del reloj En curso Sí Requisito de negocio NS-SGSI Gestión Operaciones | Requisito de negocio Garantiza que
todos los sistemas tengan hora sincronizada. Como requisito de negocio, es crítico para correlacionar logs, detectar incidentes y mantener integridad de transacciones. No suele ser mandato legal directo, pero sin sincronización adecuada, la trazabilidad de eventos se vuelve inviable. Se implementa mediante protocolos como NTP con servidores de tiempo confiables.

A.8.18 A27002-221 - A.8.18 Uso de utilidades con privilegios de sistema En curso Sí Requisito de negocio Requisito contractual | Negocio + Contractual
Controla herramientas que ejecutan comandos con altos privilegios. Negocio: previene configuraciones erróneas o maliciosas que comprometan sistemas. Contractual: auditorías externas pueden verificar que estas utilidades estén restringidas. Requiere inventario de utilidades privilegiadas, aprobación formal para su uso y registro de actividades.

A.8.19 A27002-222 - A.8.19 Instalación de software en explotación En curso Sí Requisito de negocio | Requisito de negocio Regula qué software puede
instalarse en sistemas productivos. Como requisito de negocio, evita software no autorizado que pueda introducir vulnerabilidades o conflictos. Implica listas blancas de software aprobado, procesos de cambio formal y verificación de integridad antes de despliegue.

A.8.23 A27002-226 - A.8.23 Filtrado web En curso Sí Requisito de negocio. | Requisito de negocio Implementa controles para restringir acceso a sitios web
peligrosos o no relacionados con el trabajo. Negocio: reduce exposición a malware, phishing y uso inapropiado de ancho de banda. No suele tener mandato legal, pero es una medida preventiva estándar. Requiere políticas claras, herramientas de filtrado y monitoreo de excepciones.

A.8.28 A27002-231 - A.8.28 Generación de código seguro En curso Sí Requisito de negocio Requisito contractual | Negocio + Contractual Establece
prácticas de desarrollo que minimizan vulnerabilidades desde el origen. Negocio: reduce costos de corrección y riesgos de producción. Contractual:

clientes de servicios de desarrollo exigen cumplimiento de estándares de codificación segura. Incluye revisiones de código, análisis estático y formación de desarrolladores.

A.8.29 A27002-232 - A.8.29 Pruebas seguras en el desarrollo y aceptación En curso Sí Requisito de negocio Requisito contractual | Negocio + Contractual
 Garantiza que el software se pruebe antes de producción. Negocio: detecta defectos temprano reduciendo costos. Contractual: acuerdos de entrega suelen incluir criterios de aceptación de seguridad. Requiere entornos de prueba aislados, casos de prueba de seguridad y aprobación formal antes de migración.

A.8.30 A27002-233 - A.8.30 Desarrollo externalizado En curso Sí Requisito de negocio | Requisito de negocio Aplica controles cuando el desarrollo se realiza por terceros. Como requisito de negocio, asegura que el código externo cumpla estándares internos de calidad y seguridad. Implica supervisión del proveedor, auditorías de código y cláusulas contractuales específicas sobre seguridad.

A.8.33 A27002-236 - A.8.33 Información de prueba En curso Sí Requisito de negocio Requisito contractual Requisito legal | Negocio + Contractual + Legal
 Gestiona datos utilizados en entornos de prueba. Negocio: evita contaminación de datos de producción. Contractual: clientes exigen que sus datos no se usen en pruebas sin autorización. Legal: leyes de protección de datos prohíben usar datos personales reales en pruebas sin consentimiento. Requiere anonimización o datos sintéticos.

A.8.34 A27002-237 - A.8.34 Protección de sistemas de información durante pruebas de auditoría En curso Sí Requisito de negocio | Requisito de negocio
 Asegura que las auditorías no afecten operaciones normales. Como requisito de negocio, previene interrupciones durante evaluaciones externas. Implica ventanas de mantenimiento acordadas, copias de seguridad previas y monitoreo durante las pruebas.

OBS: Los controles con los tres requisitos (negocio, contractual y legal) deben priorizarse en la hoja de ruta, ya que el incumplimiento genera riesgos simultáneos en operaciones, relaciones comerciales y cumplimiento normativo

Proceso: SUR3P EVALUACION DESEMPEÑO Y MEJORA

Propietario Del Proceso	Auditor(a)
Comité SGSI	Antonio MAMPEL MATEU

Resumen

.Indicadores,

Se revisa con periodicidad casi diaria, los accesos (logs), copias de seguridad, restauración de datos, capacidades críticas, etc.

PI-SGSI-010 Alarmas por uso de CPU:

Objetivo: Monitorear el uso de CPU en AWS para garantizar un balance entre rendimiento y costos, evitando sobreutilización o desperdicio de capacidad.

KPI-SGSI-004 Investigación de antecedentes

Objetivo: Garantizar que todas las personas ingresadas a la empresa no posean antecedentes que puedan comprometer la seguridad, reputación o cumplimiento normativo de la organización.

KPI-SGSI-007 Descuadre en el inventario

Objetivo: Detectar discrepancias entre los activos inventariados y los activos reales, cosa que puede advertir sustracciones de activos.

KPI-SGSI-008 Incidentes por cableado

Objetivo: Monitorear y reducir incidentes relacionados con el cableado de comunicaciones y de energía

KPI-SGSI-007 Descuadre en el inventario

Objetivo: Detectar discrepancias entre los activos inventariados y los activos reales, cosa que puede advertir sustracciones de activos.

Auditoría interna:

Realizada la planificación de la auditoría 12 de enero de 2026.

Programa de auditoría,30/01/2026 , Auditor interno Xavier Ferratjans, cumple con el perfil de auditor interno.

Se realiza la auditoría el 13/02/2026 y el informe. En la misma auditoría se detecta una no conformidad, y 9 observaciones.

NCm A.8.8 : Las vulnerabilidades se gestionan únicamente dentro del entorno dedicado al cumplimiento de Book&Payment. No se realiza en todo el entorno de la empresa, únicamente en entorno PCI.

Revisión por la Dirección

Reunidos: Iris Miranda Óscar Sánchez Jaume Monserrat Marta Monserrat,

La revisión por la dirección 2025 confirma que el sistema de gestión se encuentra alineado con la estrategia organizacional, gestionándose íntegramente en JIRA con trazabilidad completa de procesos, auditorías y no conformidades. La satisfacción del cliente se mide mediante tickets de postventa en Zendesk y formaciones, mientras que el análisis de riesgos se centra en información, activos y procesos, generando vulnerabilidades y oportunidades documentadas en el mapa de procesos.

Como salidas, se establece el proyecto de Sistema de Gestión Operativo 2025 con mejoras en curso para proveedores estratégicos, planificación del cambio y adecuación de recursos. Los indicadores se automatizan mediante Power BI y se estructuran OKR en ATLAS de Atlassian, vinculando cada medición a espacios de Confluence para garantizar la trazabilidad histórica y el seguimiento continuo de los objetivos estratégicos del Mindset Digital.

Mejora continua,

Se describe en los elementos de salida de la revisión por la dirección.

No conformidad y acciones correctivas

También se gestionan no conformidades en los procesos de trabajo o parte operativa, por ejemplo:

SO-109: Escalada de privilegios no autorizada dentro de la organización Por personal con capacidad dentro de TI.

Se ha solucionado Y se han despedido dos personas que tenían Acceso de alto nivel.

Incidentes de seguridad por incumplimiento de procedimientos, copias de pw sin cifrar.

A.5.10 A27002-154 - A.5.10 Uso aceptable de activos de información y otros asociados a la misma Tareas por hacer Sí Requisito de negocio NS-SGSI Normas de uso de activos. Este control define cómo clasificar y decidir si un evento de seguridad constituye un incidente real que requiere respuesta formal. Evita sobrecargar al equipo de seguridad con falsos positivos mientras asegura que incidentes reales no pasen desapercibidos. Optimiza recursos al priorizar lo que realmente importa. Criterios claros de clasificación (gravedad, impacto, tipo de activo), umbrales de decisión documentados y registros de evaluaciones realizadas.

A.5.11 A27002-155 - A.5.11 Devolución de activos Tareas por hacer Sí Requisito de negocio. Este control establece los procedimientos para manejar incidentes confirmados de manera estructurada. Este control gestiona la recuperación de todos los activos de información y otros activos cuando finaliza el empleo o cambia el rol de un usuario. Previene que ex-empleados mantengan acceso a información sensible o retengan activos físicos (laptops, tarjetas de acceso, documentos). Es crítico para evitar brechas post-empleo y proteger la continuidad operativa. Checklist formal de salida, revocación inmediata de credenciales, inventario de activos asignados y procedimiento de verificación de devolución.

A.5.24 A27002-168 - A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información En curso Sí Requisito de negocio. Este control establece la base para responder efectivamente a incidentes de seguridad antes de que ocurran. La preparación previa reduce el tiempo de respuesta y el impacto operacional cuando ocurre un incidente. Sin planificación, la organización reacciona de forma caótica, aumentando costos y daño reputacional. Documentar roles y responsabilidades, definir procedimientos de escalación, establecer canales de comunicación y realizar simulacros periódicos.

A.5.25 A27002-169 - A.5.25 Evaluación y decisión sobre los eventos de seguridad de la información En curso Sí Requisito de negocio. Este control define cómo clasificar y decidir si un evento de seguridad constituye un incidente real que requiere respuesta formal. Evita sobrecargar al equipo de seguridad con falsos positivos mientras asegura que incidentes reales no pasen desapercibidos. Optimiza recursos al priorizar lo que realmente importa. Criterios claros de clasificación (gravedad, impacto, tipo de activo), umbrales de decisión documentados y registros de evaluaciones realizadas.

A.5.26 A27002-170 - A.5.26 Respuesta a los incidentes de seguridad de la información En curso Sí Requisito de negocio. Minimiza el impacto operacional, financiero y reputacional de los incidentes. Una respuesta efectiva puede contener daños rápidamente y restaurar la normalidad. Procedimientos documentados de contención, erradicación y recuperación; equipo de respuesta designado; pruebas regulares del plan; y registro completo de cada incidente.

A.6.8 A27002-189 - A.6.8 Notificación de eventos de seguridad de la información En curso Sí Requisito de negocio. Este control establece cómo los empleados deben reportar eventos de seguridad observados o sospechados. Crea una cultura de reporte temprano que permite detectar incidentes antes de que escalen. Los empleados son la primera línea de defensa y deben sentirse seguros al reportar. Canales de reporte accesibles (email, teléfono, portal), protección contra represalias para denunciantes y procedimientos para triaje inicial de reportes.

Proceso: SUR3P SOPORTE

Propietario Del Proceso	Auditor(a)
Comité SGSI	Antonio MAMPEL MATEU
Resumen	

Recursos, descritos en objetivos y nuevos proyectos.

Competencia:

OBS: Repercutir los niveles competenciales en todos los sistemas de gestión de la organización.

Formaciones de Udemy planificadas y evaluadas para todo tipo de personal. se realizan de forma periódica para el personal formaciones de seguridad.

Concienciación : Canal de seguridad en TEAMS, se envían incidentes y mejoras recogidas en el sistema de seguridad, cada vez que se detectan.

Comunicación: a través de Dingus General desde HR, externamente con salesforce (correo del CRM) responsabilidad de Marketing

Información documentada: la documentación se gestiona con Confluence, En Jira esta la documentación del sistema. No hay documentación en papel.

A.6.4 A27002-185 - A.6.4 Proceso disciplinario En curso Sí Requisito de negocio | Requisito de negocio Establece que la organización debe tener un proceso formal para sancionar violaciones de seguridad de la información por parte del personal. Como requisito de negocio, esto disuade comportamientos negligentes o maliciosos y demuestra que la seguridad es una responsabilidad seria. Implica definir claramente las consecuencias de violaciones, documentar procedimientos y aplicar sanciones de manera consistente y justa. No suele tener mandato legal directo, pero es esencial para la cultura de seguridad interna.

A.6.5 A27002-186 - A.6.5 Responsabilidades ante la finalización o cambio de empleo En curso Sí Requisito de negocio | Requisito de negocio Define los procedimientos para gestionar el acceso y responsabilidades cuando empleados dejan la organización o cambian de rol. Como requisito de negocio, previene accesos no autorizados post-empleo y asegura transferencia adecuada de responsabilidades. Incluye revocación inmediata de credenciales, devolución de activos, actualizaciones de permisos y comunicación de nuevas responsabilidades. Es crítico para evitar brechas de seguridad por cuentas huérfanas o permisos obsoletos.

A.7.1 A27002-190 - A.7.1 Perímetro de seguridad física En curso Sí Requisito de negocio NS-SGSI Seguridad Física | Requisito de negocio Establece límites físicos alrededor de áreas que contienen información sensible. Como requisito de negocio, protege activos críticos contra acceso no autorizado, robos o sabotajes. Implica barreras físicas (muros, vallas), señalización clara de zonas restringidas y delimitación de áreas de acceso diferenciado. La implementación debe equilibrar seguridad con accesibilidad operativa.

A.7.2 A27002-191 - A.7.2 Controles físicos de entrada En curso Sí Requisito de negocio NS-SGSI Seguridad Física | Requisito de negocio Regula quién puede acceder físicamente a instalaciones y áreas sensibles. Como requisito de negocio, asegura que solo personal autorizado ingrese a zonas críticas. Incluye sistemas de identificación (tarjetas, biométricos), guardias de seguridad, registros de entrada/salida y visitas acompañadas. Los controles deben ser proporcionales al nivel de sensibilidad de cada área.

A.7.3 A27002-192 - A.7.3 Seguridad de oficinas, despachos y recursos En curso Sí Requisito de negocio NS-SGSI Seguridad Física | Requisito de negocio Protege espacios de trabajo individuales y equipos dentro de ellos. Como requisito de negocio, previene acceso no autorizado a información en escritorios, pantallas visibles o dispositivos desatendidos. Incluye políticas de escritorio limpio, bloqueo de pantallas, almacenamiento seguro de documentos y protección de equipos móviles. Es fundamental para prevenir fugas de información por descuido interno.

A.7.4 A27002-193 - A.7.4 Supervisión de la seguridad física En curso Sí Requisito de negocio | Requisito de negocio Implementa monitoreo continuo de áreas físicas mediante cámaras, sensores y alarmas. Como requisito de negocio, permite detección temprana de intrusiones o incidentes y proporciona evidencia para investigaciones. Requiere políticas de grabación, retención de footage, acceso restringido a grabaciones y revisión periódica de eventos registrados.

A.7.5 A27002-194 - A.7.5 Protección contra las amenazas físicas y ambientales En curso Sí Requisito de negocio Requisito contractual Requisito legal

NS-SGSI Seguridad Física | Negocio + Contractual + Legal Este control tiene triple motivación:

Negocio: Protege infraestructura crítica contra incendios, inundaciones, cortes eléctricos, etc.

Contractual: Clientes exigen garantías de continuidad operativa ante desastres naturales.

Legal: Algunas regulaciones sectoriales requieren planes de protección ambiental específicos. Incluye sistemas contra incendios, control climático, UPS, generadores y planes de contingencia.

A.7.6 A27002-195 - A.7.6 Trabajo en áreas seguras REVISADO Sí Requisito de negocio Requisito contractual NS-SGSI Seguridad Física | Negocio + Contractual Establece reglas específicas para personas que trabajan dentro de áreas físicamente protegidas.

Negocio: Minimiza riesgos de exposición accidental de información sensible.

Contractual: Algunos clientes requieren que su personal siga protocolos especiales en áreas compartidas. Incluye prohibición de fotografía, uso de dispositivos personales, limpieza de áreas al finalizar jornada y supervisión de visitantes.

8. INFORMACION ADICIONAL / COMENTARIOS

La auditoría se ha realizado íntegramente en remoto tal y como se ha indicado en el plan de auditoría. La herramienta de comunicación remota se propone el cliente después de recibir el plan de auditoría, se considera eficaz. MEET.

SITE SERVICE SCOPE - ANNEX A

ANNEX - SITE IN CERTIFICATION SCOPE	
*The scope is shown at site level only where it is different to the main scope for the service (as displayed in audit criteria section of the report)	
Sitios	Service/Scope}
SITIO 1: TRIPODE PARTNERS GROUP, S.L. - Galileo Galilei, 2, Edificio U, Planta baja, Local 1, 07121, PARC BIT, Palma de Mallorca, Balears España	ENAC ISO/IEC 27001:2022: Spanish: *

WWW.SGS.COM

WHEN YOU NEED TO BE SURE

