2023

5.1693 1S2

INFORME DE AUDITORÍA[1]

QUER SYSTEM INFORMÁTICA, S.L.

NORMA DE APLICACIÓN:

- ISO 9001:2015 ☐
- ISO 14001: 2015 ☐
- ISO 45001:2018 ☐
- UNE 66102:2019 ☐
- UNE 166002:2021 ☐
- ISO 27001:2013 ☒
- ISO 50001:2018 ☐
- INDICAR OTRAS* ☐

TIPO DE AUDITORIA:

INTEGRADA ☐ **CONJUNTA** ☐ **COMBINADA** ☐

• AUDITORIA CERTIFICACIÓN	☐		
• AUDITORIA SEGUIMIENTO	☒	con modificación ☐	con transferencia ☐
• AUDITORIA RECERTIFICACIÓN	☐	con modificación ☐	con transferencia ☐
• AUDITORIA EXTRAORDINARIA	☐		
• AUDITORIA AMPLIACIÓN	☐		

Fechas de auditoría	Tiempo auditoría (n º jornadas)
29 de Mayo de 2023	1

IVAC-INSTITUTO DE CERTIFICACIÓN, S.L.
CIF: B97596746
Parc Cientific de la Universitat de València. Edificio 1 (SC)
Calle Catedrático Agustín Escardino, nº 9
46980 Paterna
Teléfono: **963943905**
e-mail: **auditorias@ivac.es**

[1] El presente informe va acompañado de su Anexo con el registro de la reunión final (Anexo_Impreso AU-02-03)

2023

5.1693 1S2

ORGANIZACIÓN	
Razón Social	QUER SYSTEM INFORMÁTICA, S.L.
Email de contacto	dionisio.anton@quersystem.com; olga.sanchez@quersystem.com
Sede central	CL Andarella Nº 1, Bloque 3, Piso 3, Puerta 4 46950 Xirivella (VALENCIA)
Centros incluidos dentro del alcance	

OBRAS, INSTALACIONES O SERVICIOS VISITADOS	
	Obra ☐
	Instalación ☐
	Servicio ☐

EQUIPO AUDITOR		
Categoría	**Esquema**	**Nombre**
Auditor Jefe en cualificación	☐SGC ☐SGA ☐SGCTT ☐SGIDi ☐SST ☒SSI ☐ Otra	
Auditor	☐SGC ☐SGA ☐SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra	Jorge Edo Juan
Auditor CS	☐SGC ☐SGA ☐SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra	
Experto	☐SGC ☐SGA ☐SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra	
Evaluador	☐SGC ☐SGA ☐SGCTT ☐SGIDi ☐SST ☒SSI ☐ Otra	
Observador	☐SGC ☐SGA ☐SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra	

SGC calidad	SGA medioambiente	SGCTT tacógrafos	SGIDi investigación	SST seguridad	SSI información

REUNIONES. PARTICIPANTES DE LA EMPRESA		
Nombre	Cargo	Inicial/Auditoría
Dionisio Antón	Dirección	☐ I ☒ A
Miguel Angel Cedillo	Responsable del SGSI	☒ I ☒ A
		☐ I ☐ A
		☐ I ☐ A
		☐ I ☐ A
		☐ I ☐ A

Justificación para SGSST (ISO 45001)	
Nombre / Función	AUSENCIAS
Médico	
Representante de los trabajadores SST	
Representante servicio prevención	
Nombre / Función	ENTREVISTAS EN REMOTO
Médico	
Representante de los trabajadores SST	
Representante servicio prevención	

COMENTAR EN LA REUNION INICIAL

☒ Presentación formal del equipo auditor. Confirmación del idioma de auditoría.
☐ Aclarar el papel del experto (si procede).
☒ Aclarar el papel de observadores, consultores y otro tipo de participantes de la auditoria
☒ Confidencialidad.
☒ Confirmación datos de AU 01-01, Número de trabajadores actual de la empresa.
☒ Sala de trabajo / reuniones.
☒ Disponibilidad del personal y guías (si procede).
☒ Medidas preventivas que debe adoptar el equipo auditor

Auditoría en remoto

☐ Confirmar TICs acordadas.
☐ Confirmar Confidencialidad, seguridad de la información.
☐ Utilización copias de pantalla o de otro tipo de documentos.
☐ Envío de documentación por email.

Información general
☐ Revisión de la solicitud de certificación
☐ Revisión del alcance solicitado, definiéndolo en este momento si no está suficientemente claro
☐ Revisión de la solicitud de modificación del alcance de la certificación
☒ Revisión del alcance de la certificación concedida
☒ Revisión de las condiciones de certificación (generales y especiales)
☒ Criterios de certificación específicos
☒ Norma de evaluación (verificar las indicadas en la portada del informe).
☒ Procedimiento de actuación del IVAC ante incumplimientos en materia de legislación medioambiental. Procedimiento de actuación del IVAC ante incumplimientos en materia de legislación industrial (de producto, tales como el marcado CE, requisitos sanitarios u otras exigibles, o autorizaciones administrativas para el desarrollo de la actividad). Procedimientos del IVAC ante incumplimientos en materia de legislación de prevención de riesgos.

Metodología
☒ Métodos y procedimientos que se van a utilizar durante auditoría sobre la base de un muestreo
☒ Cómo se identifican los incumplimientos y desacuerdo con los mismos.
☒ Clasificación de los incumplimientos (Se informará cuando se identifiquen)
☒ Reunión diaria y reunión final.
☒ Informe de auditoría y recomendaciones del equipo auditor
☒ Oportunidades de mejora.
☒ Plan de acciones correctivas y comprobación de las mismas.
☐ Resultado del estudio documental previo (si se ha realizado).
☒ Auditorías de seguimiento ordinarias, de modificación de alcance y extraordinarias (metodología).
☒ Apelaciones, quejas y reclamaciones (ante el IVAC).
☒ Denuncias.
☒ Necesidad de informar de cambios que afecten al alcance de la certificación concedida.
☒ Resolución de cualquier duda que tenga la entidad.
☒ Condiciones bajo las cuales la auditoría puede darse por terminada prematuramente

Plan de auditoría
☒ Remitido. Revisar, concretar y preparar.
☐ Revisión de las NC/DESV de la auditoria anterior.

COMENTAR EN LA REUNION FINAL

☒ Presentar el Informe de auditoría.
☐ Comentar todas las no conformidades y desviaciones pendientes (comprobar que han quedado entendidas, e indicar que es por muestreo y pueden existir más desviaciones no identificadas).
☐ Comentar las oportunidades de mejora
☐ Comentar los medios de comprobación de la implantación de las acciones correctivas. (Proceso para el tratamiento de la NC/Desv. identificadas en la auditoria).
☒ Opiniones divergentes de la empresa (registrar en el informe si procede).
☐ Solicitar plan de acciones correctivas.
☐ Evaluar plan de acciones correctivas (si procede).
☐ Se entrega copia del informe de auditoría.
☒ Se remitirá copia del informe de auditoría con posterioridad.
☒ El IVAC no se lleva ninguna documentación de la empresa (salvo lo indicado a continuación).
☒ Explicar los pasos en el proceso posteriores a la auditoria.
☒ Solicitar de la empresa cualquier aclaración del proceso de certificación que pudiera tener.
☒ Solicitar quejas y reclamaciones al IVAC.
☒ Entregar impreso DG-01-05 (“**ENCUESTA DE EVALUACIÓN DE AUDITORES**”).

Se adjuntan al expediente los siguientes documentos:

☒ Plan de Auditoria, Listas de comprobación.
☒ Manual del sistema de gestión.
☒ Listado de documentos en vigor.
☐ Listado de impresos en vigor.
☐ Requisitos reglamentarios.
☒ Otros. Declaración de Aplicabilidad.

CRITERIOS DE AUDITORIA.

- Normas identificadas en la portada del informe.
- Documentación del sistema de gestión de la organización.
- Reglamentos Europeos, Normativa estatal, Autonómica y local que aplique al servicio o al producto que se realiza en la organización.
- Documentación de IVAC (según apliquen por el esquema de certificación), PAU-02, DI-018, DI-045, DI-046, DI-072.

OBJETIVOS DE LA AUDITORIA.

- la eficacia del sistema de gestión en su totalidad, a la vista de los cambios internos y externos, y su pertinencia y aplicabilidad continuas para el alcance de la certificación;
- el compromiso demostrado para mantener la eficacia y la mejora del sistema de gestión con el fin de reforzar el desempeño global;
- la eficacia del sistema de gestión en relación con el logro de los objetivos del cliente certificado y los resultados previstos del sistema (o sistemas) de gestión respectivos.
- cuando corresponda, la identificación de las áreas de mejora potencial del sistema de gestión.

La Auditoría se ha realizado a través de un muestreo por lo que pueden existir otras No Conformidades no identificadas en este informe. Las No Conformidades se refieren a incumplimientos de los requisitos de las Normas de referencia/especificaciones aplicables, de los documentos del Sistema de Gestión de la Organización o de incumplimientos legales que afectan al alcance de la certificación.

Cuando las evidencias disponibles de la auditoría indiquen que los objetivos de la auditoría no son alcanzables o sugiera la presencia de un riesgo inmediato y significativo (por ejemplo, en materia de seguridad), el Auditor jefe debe informar de este hecho al cliente y, si es posible, al IVAC para determinar las acciones apropiadas. Estas acciones pueden incluir la reconfirmación o la modificación del plan de auditoría, cambios en los objetivos de la auditoría o en su alcance, o la finalización de la auditoría.
El Auditor Jefe debe informar al organismo de certificación del resultado de las acciones tomadas.

Una auditoría de certificación de un sistema de gestión no es una auditoría de cumplimiento legal.

☒ Se cumplieron los objetivos de la auditoria de acuerdo con lo establecido en el plan de auditoría.

☐ No se cumplieron debido a:

ALCANCE DE LA CERTIFICACIÓN *(Si procede, especificar el alcance para cada uno de los centros)*
El sistema de gestión de seguridad de la información que da soporte a las actividades de: • Servicios Cloud de pago por uso en la nube. • Servicio de consultoría IT e implantación de proyectos tecnológicos. • Servicio de Comunicaciones Unificadas. • Sincronización de ficheros. • Servicio avanzado de monitorización interna y externa. • Servicio de Virtualización de escritorios.
En 27001 Versión de la Declaración de Aplicabilidad (SoA). SGSI.03 Versión 2.2 del 02/02/2022

MODIFICACIONES SOBRE EL ALCANCE DE LA CERTIFICACIÓN *(Si procede, especificar el alcance para cada uno de los centros)*
En 27001 Versión de la Declaración de Aplicabilidad (SoA).

El alcance debe establecer los tipos de productos y servicios cubiertos, y proporcionar la justificación para cualquier requisito de esta Norma Internacional que la organización determine que no es aplicable para el alcance de su sistema de gestión.

RESUMEN DE AUDITORIA

Nº DE TRAB. POR CENTRO según DI-047

(1) CAMBIOS SIGNIFICATIVOS EN EL SISTEMA DE GESTION. *(Documentación, procesos, ubicaciones, nuevas tecnologías, cambios en la infraestructura. Indicar cualquier cuestión significativa que afecte al programa de auditoría)*

No se han producido modificaciones en el sistema que afecten al programa de auditoría, manteniéndose para esta auditoría la ubicación en Calle Andarella Nº 1, bloque 3, piso 3, puerta 4. 46950 Xirivella, VALENCIA.

No se han producido modificaciones en el sistema que afecten al programa de auditoría, por lo que se mantiene el establecido inicialmente. Como único cambio reseñable ha sido la sustitución de Antonio Ferrer como responsable del SGSI por Miguel Angel Cedillo.

(2) RESOLUCIÓN ÁREAS DE INTERÉS (AI) DE FASE 1, NO CONFORMIDADES Y DESVIACIONES DE LA AUDITORÍA ANTERIOR.

NC	Cierre	Evidencias Consultadas
No se detectaron		

DESV	Cierre	Evidencias Consultadas
No se detectaron.		

(3) USO DE LA MARCA.

Se considera el reglamento de uso de la marca de entidad certificada por parte de la organización, haciendo uso de las marcas según las condiciones de utilización.

(4) ESTRUCTURA DE LA ORGANIZACIÓN. EVOLUCIÓN Y EFICACIA GLOBAL DEL SISTEMA EVALUADO. *Una declaración sobre la conformidad y eficacia del sistema de gestión, junto con un resumen de la evidencia relacionada con: la capacidad del sistema de gestión para cumplir los requisitos aplicables y lograr los resultados esperados; la auditoría interna y el proceso de revisión por la dirección; Una conclusión sobre lo apropiado del alcance de la certificación;*

4	**CONTEXTO DE LA ORGANIZACIÓN** Comprensión de la organización y de su contexto. Comprensión de las necesidades y expectativas de las partes interesadas. Determinación del alcance del sistema de gestión de la seguridad de la información. Sistema de gestión de la seguridad de la información y sus procesos.	**OK**

Comprensión de la organización y de su contexto.

QUER SYSTEM es una organización de consultoría y servicios TIC especializada en la implantación de proyectos tecnológicos que aportan a las empresas de forma integrada soluciones para la gestión empresarial. Se realizan soluciones tecnológicas 360º mediante la integración de productos de los principales desarrolladores.
Los servicios son totalmente personalizados, creando protocolos a medida para garantizar una calidad de servicio y una adecuada gestión de los clientes y recursos.
Mantiene como información documentada el SGSI.01 “Manual de Gestión de la Información”, versión 1.3 del 08/03/2021, que integra las referencias a las Normas de seguridad de la información y otras relacionadas (ISO 27001, 27017 y 27701, ENS).

En base al documento PS.16 “Procedimiento de análisis DAFO” se ha realizado el análisis de debilidades, amenazas, fortalezas y oportunidades. Se han tenido en cuenta tanto las cuestiones internas como externas que son pertinentes al propósito de empresa y la adopción de estrategias (ofensivas, defensivas, de cambio y de supervivencia). Evidencia: SGSI.07 Análisis DAFO. La fecha de la revisión es de 20/04/2023.

Se realiza un cuestionario y se realiza el cálculo de las puntuaciones de manera objetiva.
Se plantean cuestiones en el contexto externo sobre clientes, competidores, proveedores y otros factores.
En el contexto interno, sobre habilidades, estructura de la empresa y recursos.
Se han valorado las cuestiones y la última revisión del DAFO en base al procedimiento resulta que se encuentran recogidos como fortalezas y oportunidades. Ninguna de éstas se encuentra valorada para incluirse como debilidad o amenaza.

En valores de 0 a 12 (debilidades y amenazas) se consideran como factores negativos y de 13 a 24 como positivos (fortalezas y oportunidades).

Matriz DAFO

Interno	**Fortalezas** Habilidades (21) Estructura de la empresa (22) Recursos (19)	**Debilidades**
Externo	**Oportunidades** Clientes (21) Proveedores (21) Otros Factores (17)	**Amenazas** Competidores(11)

Estrategias

Estrategia ofensiva (Se usan los puntos fuertes para aprovechar oportunidades)	**Estrategia defensiva** (Se usan los puntos fuertes para tratar de evitar las amenazas)
Mis clientes están satisfechos con mis instalaciones y equipo	Dispongo de recursos (dinero) cuando los requiero
Estrategia de cambio (Se aprovechan las oportunidades para superar debilidades)	**Estrategia de supervivencia** (Se trata de reducir las debilidades para sobrevivir a las amenazas)
Sabría qué medidas tomar, en caso de cambios en la situación económica del país	Negociar con los proveedores más descuentos Hacer un estudio más exhaustivo de mis competidores

Mejora 1: Profundizar en el DAFO (bajarlo in poco de nivel), orientándolo mucho más a Seguridad de la Información. Dado que se utiliza un cuestionario para realizar el DAFO, se recomienda incluir más preguntas orientadas a la Seguridad de la información, privacidad y cloud.

Comprensión de las necesidades y expectativas de las partes interesadas.

En el Manual de Gestión (SGSI.01 Manual de Gestión) de fecha 23/05/2022, se han identificado los grupos de interés de QUER SYSTEM, así como sus necesidades y expectativas y requisitos en seguridad de la información.

Las partes interesadas son las siguientes:
- Clientes
- Proveedores
- Administración Pública
- Trabajadores
- Competencia
- Acreedores y Entidades Financieras
- Propietario de la empresa.

Se incluyen conceptos relacionados con la seguridad de la información, como preservar la confidencialidad, integridad y disponibilidad de los datos y cumplir con las normas y leyes de aplicación.
Se detallan las relaciones entre las diferentes partes interesadas y los servicios dentro del alcance.
En la revisión por Dirección se incluye la retroalimentación/comentarios que se haya podido producir por parte de las partes interesadas.

Determinación del alcance del sistema de gestión de la seguridad de la información.
Sistema de gestión de la seguridad de la información y sus procesos.

El Manual de Gestión recoge el alcance del SGSI de QUER SYSTEM para el sistema de gestión de seguridad de la información que da soporte a las actividades de:
- Servicios Cloud de pago por uso en la nube.
- Servicio de consultoría IT e implantación de proyectos tecnológicos.
- Servicio de Comunicaciones Unificadas.
- Sincronización de ficheros.
- Servicio avanzado de monitorización interna y externa.
- Servicio de Virtualización de escritorios.

El centro de trabajo se ubica en c/ Andarella Nº 1, bloque 3, piso 3, puerta 4, en Xirivella (Valencia).
Según “Declaración de Aplicabilidad (SoA)”, se encuentra vigente para esta auditoría la versión 2.2 de 02/02/2022. En ella, se establecen los objetivos de control y controles aplicables y no aplicables al SGSI.
Se consideran no aplicables, en base a la justificación definida, los siguientes controles:

- A.8.3.3
- A.14.2.1
- A.14.2.6
- A.14.2.7
- A.14.3.1

La organización dispone de información documentada (Manual de Gestión, Procedimientos, Registros) para apoyar la operación de sus procesos y asegurarse de que los procesos se realizan según lo planificado.

5-6	**LIDERAZGO Y PLANIFICACION** Liderazgo y compromiso. Política, Establecimiento de la política de SGSI, Comunicación de la política. Roles, responsabilidades y autoridades en la organización. Apreciación y Tratamiento de los riesgos de seguridad de la información (Definición de criterios y controles). Objetivos de la seguridad de la información y planificación para lograrlos.	**OK**

Liderazgo y compromiso.
Se mantiene entrevista con Dionisio Antón, que representa la Dirección de QUER SYSTEM y coordina las distintas áreas de la empresa en la reunión de cierre de la auditoría.

El liderazgo y el compromiso de la alta dirección con el sistema de gestión se demuestra asegurando el establecimiento de la política y de los objetivos, la integración del sistema de gestión en los procesos de la organización, promoviendo el enfoque basado en riesgos, impulsando la mejora y asegurando la disponibilidad de los recursos necesarios para el desarrollo del sistema y de las propias actividades.
Se transmite al personal la importancia de satisfacer tanto los requisitos del cliente como los legales y reglamentarios.

Política, Establecimiento de la política de SGSI, Comunicación de la política.

La "Política de Seguridad de la Información" (SGSI.01-07) se mantiene vigente en QUER SYSTEM en versión 3 del 22/03/2021.
La política se encuentra definida en base a los principios de confidencialidad, integridad, disponibilidad y legalidad e incluye los requisitos exigidos por la Norma de referencia. Se considera adecuada al propósito y contexto de la organización como apoyo a su dirección estratégica.
Internamente se ha comunicado al personal mediante correo electrónico.
Para el resto de las partes interesadas se ha considerado incluirla en la web corporativa segura en la dirección https://quersystem.com/wp-content/uploads/2022/06/Politica-de-seguridad-ISO27001.pdf.
Se encuentra disponibles las políticas ISO, ENS y calidad.

Roles, responsabilidades y autoridades en la organización.

La seguridad de la información en QUER SYSTEM es coordinada por parte del Comité de Seguridad, integrado por los Responsables de la Información, del Servicio, de Seguridad y del Sistema.
En el Manual de Gestión se recogen las principales funciones y responsabilidades.
Los distintos puestos de trabajo y responsabilidades se encuentran representados en el organigrama de la organización (SGSI.01-03).
Se dispone, igualmente, de las fichas de perfil profesional (FO.PS.11-04).", con las funciones y responsabilidades para cada perfil y de manera específica en materia de seguridad de la información.
Antonio Ferrer era el anterior Responsable SGSI y ha sido sustituido durante este año por Miguel Angel Cedillo.
En los distintos procedimientos se describen las responsabilidades sobre el aspecto referenciado y tratado en cada caso.

Los miembros del Comité de Seguridad son los siguientes:
Funciones y Responsabilidades aparece que los miembros del comité son los siguientes:
- Responsable del Servicio, de la Información y de Seguridad: Director General.
- Responsable del Sistema: Responsable de TI.

En la revisión por dirección: Versión: 3.2. Fecha: 24/5/2023.
Se nombran como:
- Dirección de la entidad --> Dionisio Anton
- Responsable información --> Dionisio Anton
- Responsable de servicio --> Dionisio Anton
- Responsable de seguridad --> Antonio Ferrer
- Responsable de sistema → Miguel Angel Cedillo

Ambos documentos y nombramientos han sido aprobados por la Dirección de QUER SYSTEM.

Observación 1: Modificar el punto 4.4.2.- 4.4.2. Roles, para incluir los miembros correctos, de cara a evitar discrepancias se recomienda disponer de un único repositorio donde se incluyan los diferentes cargos.

Apreciación y Tratamiento de los riesgos de seguridad de la información (Definición de criterios y controles).

Se revisa el documento SGSI.04 "Análisis y gestión de riesgos" y procedimiento PS.01 "Análisis de riesgos", con la metodología para identificación de activos, valoración y gestión de riesgos.
Se dispone de inventario de activos con la siguiente identificación:
- [B] Activos esenciales ([SE] Servicios esenciales, [IN] Información Esencial)
- [E] Equipamiento ([SW] Aplicaciones, [HW] Equipos, [COM] Comunicaciones)
- [SS] Servicios subcontratados
- [L] Instalaciones
- [P] Personal

El análisis de riesgos se realiza sobre los activos identificados dentro del alcance, con nombre, tipo y valoración. La valoración se hace en cada una de las dimensiones de la seguridad (C, I, D).

Se calcula el riesgo en función de la probabilidad de que se materialice una amenaza y el impacto que supondría esa ocurrencia.
Se estiman las amenazas y vulnerabilidades, con la valoración de la degradación, en base a la metodología de análisis y gestión de riesgos Magerit.
El análisis de riesgos permite conocer con detalle el sistema, con los activos y su valoración, así como las amenazas a las que está expuesto.
El riesgo residual es el que presentan los activos tras implantar los controles previstos.
El Comité de Seguridad aprueba el valor del riesgo aceptable y realiza la aceptación del riesgo residual.
Se ha definido como el nivel de riesgo aceptable aquel inferior a 6.

El tratamiento de riesgo se centra en seleccionar medidas de seguridad para controlar las amenazas

Objetivos de la seguridad de la información y planificación para lograrlos. Planificación de los cambios.

Se revisa el documento SGSI.05 “Plan de Mejora”, para planificar la implantación de medidas técnicas y organizativas para reducir los riesgos SI.
Se evidencian los anexos con la planificación de objetivos. Para 2022 se establecieron los siguientes:

- Optimización de la sensibilización y concienciación del personal en os requisitos de la Norma.
- Mejora de la capacidad de los servidores que soportan el servicio.
- Implantar el doble factor de autenticación el 90% de los empleados.

Para cada objetivo se detallan las tareas/acciones, dimensión afectada, plazo, responsable, recursos, prioridad, activos afectados e indicador asociado, así como los controles relacionados.

A fecha de esta auditoría se ha observado que los anteriores objetivos se completaron con éxito.

Para el 2023, se han planteado los siguientes objetivos:

- Optimización de la sensibilización y conciencación del personal en los requisitos de la norma de referencia.. Formación de los empleados en el ENS (RD 311/2022)
- Mejora de la capacidad de los servidores que soportan el servicio
- Implementar en toda la infraestructura nuevo sistema de copias de seguridad

QUERSYSTEM	01/02/2023	SGSI.04-01 Anexo I Objetivos					Documento de uso interno	Ver 2023		
TAREAS	DIMENSIÓN AFECTADA	PLAZO	RESPONSABLE	RECURSOS	PRIORIDAD	ACTIVOS AFECTADOS	INDICADOR ASOCIADO	SEGUIMIENTO 1º SEMESTRE	SEGUIMIENTO 2º SEMESTRE	CONTROLES RELACIONA
OBJETIVO 1	Optimización de la sensibilización y concienciación del personal en los requisitos de la norma de referencia. Se pretende que el 50% de los usuarios estén sensibilizados a los requisitos del sistema de gestión según l									
Formacion de los empleados en el nuevo ENS	Disponibilidad	01/12/23	Responsable de Seguridad	Horas Responsable de Seguridad Coste del producto	Baja	Servidores Servicios				mp.per.4 Gestión de personal
Hacer el curso Nuevo ENS de CCN		Dic. De 2023								
OBJETIVO 2	Mejora de la capacidad de los servidores que soportan el servicio									
Adquisición de servidores	Disponibilidad	01/12/23	Responsable de Seguridad	Horas Responsable de Seguridad Coste del producto	Baja	Servidores Servicios				op.pl.3 Adquisición de nuevos component
Estudiar la capacidad necesaria		Dic. De 2023								
Seleccionar producto que se desea adquirir		Dic. De 2023								
Realizar la compra		Dic. De 2023								
Puesta en producción		Dic. De 2023								
OBJETIVO 3	Implementar en toda la infraestructura nuevo sistema de copias de seguridad									
Implentar nuevo sistema de copias de seguridad	Disponibilidad	01/12/23	Responsable de Seguridad	Horas Responsable de Seguridad Coste del	Media	Servidores Servicios				mp.info.9 Proteccion de la información
Implementar en KIO		Dic. De 2023								
Implementar en HET		Dic. De 2023								
Implementar en WALL		Dic. De 2023								

Actualmente la organización se encuentra realizando los planes de acción de los 3 objetivos anteriores.

7	**PROCESOS DE APOYO** Personal. Conocimiento de la organización. Competencia. Toma de Conciencia. Comunicación. Información documentada / Control de la documentación.	OK

Personal. Conocimiento de la organización. Competencia. Toma de Conciencia.

Las clausulas 7.1, 7.2, 7.3 y 7.4 no se revisan en esta auditoría.

Comunicación.

Se revisa el documento SGSI.01-01 “Plan de comunicación”.
Se enumeran los destinatarios de las comunicaciones para los distintos tipos y vías de comunicación, responsable y periodicidad.
Se realizan reuniones informativas todas las semanas de manera informal y se planifican los trabajos.
Por el tamaño reducido de la empresa, se trata de comunicaciones informales y no se deja registro mediante acta.
Para las comunicaciones más formales, se trabaja con documentos firmados y correo electrónico.

Se dispone de firmas digitales individuales y personales para la firma de documentos.
En la operativa se utiliza la herramienta de ticketing. También, con los clientes.

Información documentada / Control de la documentación.

Se observa que se dispone de un procedimiento de clasificación de la información en el que se establecen los criterios de definición de la categoría de la información gestionada por la organización.
Se han definido las siguientes categorías:

- PUBLICOS o abiertos: Divulgación externa
- INTERNOS o privados: Información de uso interno
- RESTRINGIDO: No divulgación autorización expresa
- CONFIDENCIAL: Información de alto valor para la organización.

Se revisan el documento SGSI.01-02 Clasificación de la información v1.0 de fecha 16/01/2020.

En el procedimiento se distinguen los siguientes tipos de documentos:
Documentación de RRHH. Confidencial
Documentación de Clientes. Uso Interno
Información Pública/Comercial. Uso Público

Para cada uno de los documentos anteriores se establecen una serie de indicaciones para la gestión de la documentación en papel y la documentación en soporte electrónico.

8	**PROCESOS DE PLANIFICACIÓN PARA TODOS LOS PROCESOS DE OPERACIÓN** Planificación y control operacional - Definición de los procesos de Seguridad de la información.	**OK**

Planificación y control operacional - Definición de los procesos de Seguridad de la información.

Este proceso se gestiona por la Dirección en apoyo con los responsables.
Cualquier cambio o necesidad es definido en la planificación estratégica o en la revisión del sistema y se trata en el Comité de Seguridad.
El SGSI controla los cambios a través de su procedimiento PS.10 “Gestión del SGSI”.
Los requisitos del negocio son validados por la Dirección y responsables.
En relación con la seguridad de la información se dispone de las políticas específicas recogidas en los procedimientos (PS.xx).
La sistemática para la evaluación de riesgos se realiza en base al documento SGSI.04 “Análisis y gestión de riesgos” y procedimiento PS.01 “Análisis de riesgos”.

8	**PROCESOS DE GESTIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** Apreciación de los riesgos de seguridad de la información (Declaración Aplicabilidad - actualización). Tratamiento de los riesgos de seguridad de la información (Plan de tratamiento RSI - desarrollo y seguimiento).	**OK**

Apreciación de los riesgos de seguridad de la información (Declaración Aplicabilidad - actualización).

Esta cláusula no corresponde revisarlo en esta auditoría.

Tratamiento de los riesgos de seguridad de la información (Plan de tratamiento RSI - desarrollo y seguimiento).

Se dispone de un documento: SGSI.04 Anexo III Salvaguarda de los servicios., donde se incluyen las salvaguardas definidas para los riesgos identificados en los documentos: SGSI.04 Anexo II Informe de Análisis y Gestión de Riesgos, SGSI.04 Anexo I Análisis de Riesgo servicio Cloud. A fecha de esta auditoría se mantienen los riesgos definidos en el año 2022.

Mejora 2: Se recomienda, para facilitar la evolución entre un año y el siguiente de los Riesgos y de los Planes de Tratamiento de las correspondientes salvaguardas, pasar el análisis de Riesgos y sobre todo el PTR de Word a documentos de excel, lo que facilita la comparativa entre un año y el siguiente. De esta forma también se está más en línea con lo exigido por el ENS en relación con este control.

9	**PROCESOS DE EVALUACIÓN DEL DESEMPEÑO** Definición de indicadores (seguimiento, medición, análisis y evaluación). Auditorías internas. Revisión por la Dirección.	OK

Definición de indicadores (seguimiento, medición, análisis y evaluación).

Se revisa el procedimiento PS.10 “Gestión del SGSI”.
QUER SYSTEM ha definido para la evaluación del desempeño de sus procesos el seguimiento a través de métricas e indicadores, según registro FO.PS.10-04. Mantiene definidos los siguientes:
- Incidentes de seguridad con pérdida de información que se ha recuperado.
- Incidentes de seguridad con pérdida de información que no se ha recuperado.
- Tiempo de resolución de incidencias que afectan a las aplicaciones.
- Trabajadores que han recibido formación en materia de seguridad.
- Incidentes de seguridad tratados.
- Tiempo empleado para cerrar el 50% de los incidentes.
- Tiempo empleado para cerrar el 90% de los incidentes.
- Incidentes derivados de proveedores de Cloud.
- Pruebas de continuidad realizadas satisfactoriamente.
- Duración de interrupciones de servicio.
- Porcentaje de empleados que mejoran sus competencias en los servicios o sistemas de información.

El resultado de los indicadores se encuentra dentro de los rangos definidos en todos los casos.

En cada caso se establece la métrica, frecuencia, fórmula, indicador (valor objetivo) y las mediciones.
Se evidencian los datos registrados durante 2022 y los del primer trimestre de 2023.

Observación 2: Incluir en los indicadores los correspondientes a la eficiencia en horas y presupuesto del PACS de resolución de la certificación en el ENS.

Auditorías internas.

Recogidas conforme al procedimiento PS.10 “Gestión del SGSI”.
Se revisa el plan de auditorías, según registro FO.PS.10-06. En la planificación están incluidas las auditorías internas y externas de ISO 27001, 27017 y 27701 y ENS, con las fechas previstas y la entidad auditora.
Las relativas a las Normas ISO de seguridad de la información se han planificado para mayo 2023 por parte de HILVAN Consultores. El auditor Patricio Quilez de la empresa consultora ha realizado la auditoría interna los días 16/05/2023 para todo el alcance definido.
En la auditoría no se han detectado no conformidades.

Revisión por la Dirección.

De acuerdo con el procedimiento PS.10 “Gestión del SGSI”, se ha realizado la revisión por Dirección.
El informe se encuentra documentado con fecha 24/05/2023, según FO.PS.10-03”.

A fecha 25/05/2023 se ha actualizado el contenido con la inclusión de los resultados de la auditoría interna. El acta incluye las consideraciones y decisiones y acciones requeridas como entradas y salidas por la Norma de referencia en este apartado.
Como oportunidades de mejora se registra un “Plan de Mejora 2023”, SGSI.05 Plan de Mejora 2023. En el apartado 9, se detallan, para cada una de las acciones definidas, los plazos y recursos necesarios para su efectiva implantación, así como el responsable de su seguimiento

10	**PROCESO DE MEJORA** No conformidades, Acción correctiva. Mejora continua.	**OK**

No conformidades, Acción correctiva. Mejora continua.

En base a lo establecido en el procedimiento PS.10, se dispone de documento de acciones correctivas, según registro FO.PS.10-09.
Los incumplimientos se identifican por la Norma afectada, origen y grado. Se identifica la fecha, descripción, análisis de causas, acciones, responsable, seguimiento, verificación de la eficacia y cierre.
De 2021 se Identificaron, trataron y cerraron 2 NC internas.
En 2022 se registraron 2 NC. Una, relativa a alarma de monitorización por necesidad de aumento de capacidad. Otra, por actualización de SS.OO. en una migración de plataforma de correo. Ambas se encuentran cerradas.
Recientemente se ha realizado una auditoría de certificación del Esquema Nacional de Seguridad, en la que se han detectado 6 no conformidades y 3 Observaciones. En los casos de las no conformidades se ha enviado el PACS, al auditor y revisor para su valoración.

- No se dispone de evidencia de conocimiento y aceptación de la Normativa de Seguridad de la Información por parte de los empleados de la organización.
- No se observa la identificación de salvaguardas aplicadas para la mitigación de los riesgos identificados.
- La definición de los PTR no permite una gestión adecuada de los mismos al no disponer del detalle de las acciones concretas a materializar para la mitigación de los riesgos a tratar.
- No se dispone de un Procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.
- Para conocer la eficiencia del sistema de seguridad en relación con los recursos consumidos, en términos de horas y presupuesto.
- No se informa a los colaboradores del deber de confidencialidad de forma indefinida, incluyendo a la posterioridad de la propia prestación laboral.

Adicionalmente a estas no conformidades se han identificado por parte del auditor del ENS 3 Observaciones:

- El proceso de adquisición de componentes se basa en la gestión de proveedores debido a la naturaleza de la organización, si bien debería estar debidamente procedimentado el análisis previo en caso de adquisición de material propio de la organización.
- Se observan algunos documentos del SGSI que no siguen las reglas de etiquetado establecidas.
- Se observa en la información pública de la organización ciertos documentos puntuales que disponen de información de metadatos.

Anexo A	CONTROLES ANEXO A	OK

Cada categoría principal de controles de seguridad contiene un objetivo de control que establece qué es los que se quiere conseguir y uno o más controles que pueden ser aplicados para conseguir el objetivo de control. De este modo, y según el plan de auditoría establecido, se procede a la revisión de los siguientes:

A.5. Política de Seguridad de la Información

A.5.1 Directrices de gestión para la seguridad de la información
A.5.1.1 Políticas para la seguridad de la información
El Manual de Gestión (SGSI.01) recoge los apartados de la Norma ISO 27001 siguiendo la estructura de la misma. La Política de seguridad de la información (SGSI.01-07) se encuentra definida y disponible como información documentada.
La Política de seguridad de la información (SGSI.01-07) se mantiene vigente en versión 3 del 22/03/2021.
Como documentos independientes se dispone de un conjunto de Procedimientos de Seguridad (PS.xx) en materia de seguridad de la información.
La documentación del sistema se encuentra compartida en NextCloud. La operativa, en Confluence.

A.5.1.2 Revisión de las políticas para la seguridad de la información
Se revisan las políticas en la revisión por dirección que se ha realizado recientemente.

A.6. Organización de la seguridad de la información

A.6.1 Organización interna
A.6.1.1 Definición y asignación de roles y responsabilidades relativas a la seguridad de la información
A.6.1.2 Segregación de tareas
A.6.1.3 Contacto con las autoridades
A.6.1.4 Contacto con grupos de interés especial
A.6.1.5 Seguridad en la gestión de proyectos

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.6.2 Los dispositivos móviles y el teletrabajo
A.6.2.1 Política de dispositivos móviles
Se dispone de la normativa: NP.01 Dispositivos Móviles v1, donde se precisa el uso de antivirus, y la adecuada gestión de las APPs por parte de los usuarios.

El acceso remoto es autorizado por defecto debido a la tipología de relación laboral que se mantiene en la organización que combina presencialidad con trabajo a distancia.

A.6.2.2 Teletrabajo
El acceso remoto es autorizado por defecto debido a la tipología de relación laboral que se mantiene en la organización que combina presencialidad con trabajo a distancia.

A.7. Seguridad relativa a los Recursos Humanos

A.7.1 Antes del empleo
A.7.1.1 Antecedentes
A.7.1.2 Términos y condiciones de contratación

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.7.2 Durante el empleo

A.7.2.1 Gestión de las responsabilidades

Para el personal se define en los propios perfiles del puesto de trabajo y se comunican en las acciones formativas. Para los proveedores se establecen las responsabilidades en los contratos firmados y, en particular, en el clausulado para confidencialidad y protección de datos.

Se evalúa el documento FO.PS.11-04 Perfil Profesional v2 en el que se establecen las responsabilidades en materia de Seguridad de la Información para los diferentes perfiles existentes en la organización, a saber:

- Comercial
- Técnico Soporte N1
- Responsable de Nivel 1
- Técnico Soporte N2
- Responsable de Soporte de Nivel 2
- Responsable de Sistemas / Seguridad
- Técnico de Sistema
- Administrativo/a
- Gestión de Proyectos / Servicios
- Responsable de la Información

Se revisa el perfil de Responsable de Nivel 1 de Soporte, donde se comprueba que se documenta la formación necesaria, la experiencia requerida, otras habilidades y las Responsabilidades en materia de Seguridad de la Información.

Se evalúa la existencia de FO.PS.11-05 Compromiso de Confidencialidad v1 que informa de las obligaciones y deber de confidencialidad, así como la existencia de medidas disciplinarias ante posibles incumplimientos. Se comprueba la evidencia de la firma de documento de confidencialidad por parte de Miguel Angel Cedillo de fecha 11/02/2022.

A.7.2.2 Concienciación, formación y capacitación en seguridad de la información

Concienciación:

Se observa en el canal interno de comunicación de la organización que se llevan a cabo labores de concienciación de forma recurrente en relación a la normativa de seguridad y la identificación y gestión de incidentes de seguridad.

Se evidencia comunicación relativa a las Buenas prácticas de seguridad que recogen aspectos relacionados con la normativa de seguridad.

Formación:

La organización mantiene registro de los certificados de formación emitidos por organizaciones externas.

La organización dispone de un plan anual de formación, se evidencia documentos Plan anual formación 2022 y Plan anual formación 2023.

Se evalúa ejemplo de formación de Andy Joel Da Silva.

Una vez finalizada la formación se lleva a cabo una evaluación, mediante test, de los conocimientos adquiridos durante la misma con objeto de valorar la eficacia de las acciones formativas realizadas.

A.7.2.3 Proceso disciplinario

Viene recogido en el documento NS.01 Normativa de Seguridad de la Información apartado 15 Incumplimiento de la normativa.

Todos los usuarios de QUER SYSTEM están obligados a cumplir lo prescrito en la presente Normativa de Seguridad de la Información.

En el supuesto de que un usuario no observe alguna de los preceptos señalados en la presente Normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.

A.7.3 Finalización del empleo o cambio en el puesto de trabajo

A.7.3.1 Responsabilidades ante la finalización o cambio de puesto de trabajo

La baja de trabajadores se determina en ficha de proceso PS.03 Control de Acceso v1.1 de 21/02/2023.

Se revocan los derechos de acceso, suspensión de credenciales, retirada de activos, se recuerda al empleado su compromiso de confidencialidad.

El proceso de baja de usuarios se realiza con una notificación del responsable del usuario informando de la baja del mismo. Dicha petición es aprobada por el Responsable de Seguridad y asignada al área de SysAd (Administrador de Sistemas) para su ejecución y eliminación del usuario en el Centro de control de usuarios y aquellos sistemas / certificados que estuviesen dados de alta.
Los usuarios quedan en un estado deshabilitado con objeto de garantizar la trazabilidad de las acciones realizadas.

Observación 3: Como viene recogida en la no conformidad 6 identificada en la auditoría del ENS se recomienda tanto para los nuevos como para los antiguos empleados, la firma de un nuevo documento de confidencialidad, donde se precise un periodo de tiempo de varios años de mantener la confidencialidad de la información, después de haber abandonado la empresa.

A.8. Gestión de activos

A.8.1 Responsabilidades sobre los activos
A.8.1.1 Inventario de activos
A.8.1.2 Propiedad de los activos
A.8.1.3 Uso aceptable de los activos
A.8.1.4 Devolución de activos

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.8.2 Clasificación de la información
A.8.2.1 Clasificación de la información
Se observa que se dispone de un procedimiento de clasificación de la información (SGSI.01-02 Clasificación de la información v1.0) en el que se establecen los criterios de definición de la categoría de la información gestionada por la organización.
Se han definido las siguientes categorías:

- PUBLICOS o abiertos: Divulgación externa
- INTERNOS o privados: Información de uso interno
- RESTRINGIDO: No divulgación autorización expresa
- CONFIDENCIAL: Información de alto valor para la organización.

La organización no dispone de soportes físicos de información. Por soportes físicos de información se entiende entre otros Pendrives, Discos duros externos, NAS, papel, etc…

Evidencias: Se toma una muestra de diversos documentos, donde se comprueba que en el pie de página, aparece indicada la categoría del documento. SGSI-01 Manual de Gestion de la Información (categoría confidencial), SGSI.01-05 Política de seguridad (Público), SGSI.05 Plan de Mejora 2023 (categoría confidencial).
PS.09 Protección de la Información v1.0 de 17/01/2020

A.8.2.2 Etiquetado de la información
En el encabezado de los documentos, y en el nombre se identifican los distintos documentos que forman parte del SGSI.
Evidencias: SGSI-01 Manual de Gestion de la Información (Código: SGSI.01), SGSI.05 Plan de Mejora 2023 (Código: SGSI.05)

A.8.2.3 Manipulación de la información
PS.09 Protección de la Información v1.0 de 17/01/2020, en el punto 3.1.3.3 Tratamiento de la información se indican como proceder en función de la categoría del documento y el tipo de información manejada (papel, formato electrónico).

A.8.3 Manipulación de soportes
A.8.3.1 Gestión de soportes extraíbles
A.8.3.2 Destrucción de los soportes
A.8.3.3 Soporte físico en tránsito

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.9. Control de acceso

A.9.1 Requerimientos de la empresa para el control de acceso
A.9.1.1. Política de control de acceso
A.9.1.2. Acceso a la red y a los servicios de red

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.9.2 Gestión de acceso de usuarios
A.9.2.1 Registro y baja de usuario
PS.03 Control de Acceso v1.1 de 21/02/2023
El proceso de alta y baja de usuarios se realiza con una notificación del responsable del usuario informando de la alto o baja del mismo. Dicha petición es aprobada por el Responsable de Seguridad y asignada al área de SysAd (Administrador de Sistemas) para su ejecución y alta o eliminación del usuario en el Centro de control de usuarios y aquellos sistemas / certificados que estuviesen dados de alta.
Evidencias: Ticket JIRA #MON-1132 Baja de Shrrah Castillo.
Los usuarios quedan en un estado deshabilitado con objeto de garantizar la trazabilidad de las acciones realizadas.

A.9.2.2 Provisión de acceso de usuario
Para la gestión de la información e infraestructura centralizada, dichos accesos de usuario son gestionados desde la consola de gestión de usuarios, GLUU, en la cual se dispone de características de seguridad para proteger los recursos del sistema.

A.9.2.3 Gestión de privilegios de acceso
Cada usuario deberá estar asociado a un perfil, de acuerdo a las tareas que desempeña en la organización, definido por su responsable directo. Cada uno de estos perfiles dispondrá de unos determinados permisos y verá restringido su acceso a Información y sistemas que no le son necesarios para las competencias de su trabajo.

A.9.2.4 Gestión de la información secreta de autenticación de usuario
Las contraseñas siguen el siguiente patrón: tamaño mínimo de la contraseña 8 caracteres, de los cuales 2 son mayúsculas, 2 minúsculas, 1 signo de puntuación 1 carácter numérico. Histórico contraseñas: 5, caducidad de la contraseña: 90 días.
Se dispone de doble factor para accesos desde el exterior.

Mejora 4: La longitud mínima de las contraseñas admitida es de 8 caracteres, se recomienda subir la longitud de la contraseña mínimo a 12 caracteres. Actualmente una contraseña de tan sólo 8 caracteres se considera insegura.

A.9.2.5 Revisión de los derechos de acceso de usuario
Mediante la consola ZABBIX se disponen de supervisión de los registros de actividad de los sistemas de información críticos de la organización, los cuales generan alertas a los administradores ante la materialización de patrones anormales de comportamiento de dichos logs.
Se dispone de un agente Zabbix instalado en toda la infraestructura crítica de la organización que analiza de forma permanente la actividad del sistema, incluyendo servicios, comunicaciones, usuarios, procesos, etc… La consola principal recoge toda la actividad mencionada y la analiza en base a unas reglas pre-definidas que generan alertas tempranas de identificación de incidentes así como bloquean las posibles amenazas que pudiesen generar (interrumpen el servicio, bloquean procesos, etc…).
Se revisa, por parte del auditor la consola de administración.

A.9.2.6 Cese o reasignación de los derechos de acceso
Evidencias: Ticket JIRA #MON-1132 Baja de Shrrah Castillo.
Los usuarios quedan en un estado deshabilitado con objeto de garantizar la trazabilidad de las acciones realizadas

A.9.3 Responsabilidades del usuario
A.9.3.1 Uso de la información secreta de autenticación
En la normativa NS.01 Normativa de Seguridad de la Información, vienen indicadas las indicaciones a cumplir por parte de todos los empleados en materia de contraseñas (apartado 7 Identificación y autenticación):

- Código único por usuario
- Prohibición de revelar la contraseña a otros usuarios
- Notificación al área de Sistemas ante la sospecha de que sus credenciales puedan estar siendo utilizadas por otros usuarios.

A.9.4 Control de acceso a sistemas y aplicaciones
A.9.4.1 Restricción de acceso a la información
A.9.4.2 Procedimientos seguros de registro e inicio de sesión seguro
A.9.4.3 Sistema de gestión de contraseñas
A.9.4.4 Uso de utilidades con privilegios del sistema
A.9.4.5 Control de acceso al código fuente

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.10. Criptografía

A.10.1 Controles criptográficos
A.10.1.1 Política de uso de los controles de criptográficos
A.10.1.2 Gestión de claves
Existen tres tipos de controles criptográficos. SSL para web, conexiones VPN, cifrado de disco para dispositivos portátiles y certificados FNMT.
Las webs disponen de certificado SSL.
Se utiliza el software Open VPN para el establecimiento de comunicaciones en redes fuera del dominio de seguridad. La autenticación de dichas comunicaciones se realiza en base a llaves criptográficas generadas por la propia organización en base a certificados de usuarios unívocos.
La organización hace uso de claves personales emitidos por la FNMT, no llevando a cabo gestión de generación de claves. El uso del certificado requiere de la introducción de contraseña personal.

A.11. Seguridad física y del entorno

A.11.1 Áreas seguras
A.11.1.1 Perímetro de seguridad física
A.11.1.2 Controles físicos de entrada
A.11.1.3 Asegurar las oficinas, despachos e instalaciones
A.11.1.4 Protección contra las amenazas externas y de origen ambiental
A.11.1.5 Trabajo en áreas seguras
A.11.1.6 Áreas de acceso público y de carga y descarga

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.11.2 Seguridad de los equipos
A.11.2.1 Emplazamiento y protección de equipos
La infraestructura crítica de la organización se encuentra distribuida en 3 CPDs de forma que se pueda distribuir la carga y, a su vez, sirvan de sistemas de respaldo mallado entre los mismos.
La organización se apoya en dichos proveedores para el cumplimiento del presente control, al no disponer de infraestructura crítica en las oficinas de la organización.
Los proveedores son KIO (Murcia), Walhalla (Castellón), Hetzner (Alemania). Los dos primeros disponen de Certificado ENS nivel Alto y el tercero, al no ser español, dispone de ISO 27001.
KIO Networks España (ENS ALTO)

A.11.2.2 Instalaciones de suministro
En las oficinas de la organización se disponen de luces de emergencia que cumplen con lo indicado en la normativa correspondiente.

A.11.2.3 Seguridad del cableado
Se cuenta con separación de líneas de corriente eléctrica y datos. Hay cableado normalizado de red desde los switches a los puestos de trabajo. El cableado va protegido mediante canaleta.

A.11.2.4 Mantenimiento de los equipos
Se dispone de medios de protección contra incendios. Se comprueba que los extintores están revisados y mantenidos por empresa proveedora Guipons de forma correcta. Última revisión 12 de Enero del 2023.
El mantenimiento de los equipos se realiza por parte del Administrador TI

A.11.2.5 Retirada de materiales propiedad de la empresa
A fecha de la auditoría no se ha producido retirada de Sistemas de Información propiedad de la empresa.

A.11.2.6 Seguridad del equipamiento fuera de la oficina
El uso de dispositivos móviles se establece en la normativa NP.01 Dispositivos Móviles v1.0 de 18/07/2019.
En la autorización de utilización de dispositivos móviles propiedad de la organización se establece el procedimiento de actuación ante hurto y/o perdida de los dispositivos.
La conexión desde el exterior de las instalaciones de la organización se realiza mediante conexión VPN.
Los equipos disponen de discos cifrados

A.11.2.7 Reutilización o eliminación segura de equipos
En el SGSI.01 Manual de Gestión, vienen directrices relacionadas con este control.
Los soportes reutilizables cuya información ya no se necesite deberá borrarse, siempre que se cuente con la autorización precisa. Esta eliminación debe hacerse de forma segura para que los datos que contiene no se filtren a otras personas. Algunos procedimientos de destrucción que se consideran adecuados son la incineración, el triturado o vaciamiento de los soportes para que sean usados en otra aplicación dentro de QUER SYSTEM. A fecha de la auditoría, no se ha eliminado ningún ordenador.

A.11.2.8 Equipos de usuario desatendido
La pantalla se bloquea tras 15 minutos un tiempo de inactividad y se requiere credenciales para su reactivación. El bloqueo del equipo se realiza en cualquier caso en que el usuario se ausente de su puesto.

A.11.2.9 Política puesto de trabajo despejado y de escritorio limpio
Se permite el uso de la información con la que se está trabajando en el momento, pero no se autoriza la acumulación de documentación en la mesa.
La información documentada se guarda en lugares seguros y bajo llave. En las zonas de atención al público no se encuentra documentación desatendida. Durante la visita a las instalaciones se ha podido observar que los puestos de trabajo se encuentran delimitados y con orden y limpieza.
En las bandejas de las impresoras/fotocopiadoras no se ha observado documentación pendiente de recogida o desatendida.

A.12. Seguridad de las operaciones

A.12.1 Procedimientos y responsabilidades operacionales
A.12.1.1 Documentación de los procedimientos de operación
A.12.1.2 Gestión de cambios
A.12.1.3 Gestión de las capacidades
A.12.1.4 Separación de los recursos de desarrollo, prueba y operación

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.12.2 Protección contra software malicioso (malware)
A.12.2.1 Controles contra el código malicioso

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.12.3 Copias de Seguridad
A.12.3.1 Copias de seguridad de la información

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.12.4 Registros y supervisión de eventos
A.12.4.1 Registro de eventos
En el PS02 Procedimiento de Seguridad Lógica v.3.2 de 21/02/2023 se establece la necesidad de incorporar registros de la actividad de los usuarios en su punto 3.5.7.
Mediante la consola ZABBIX se disponen de supervisión de los registros de actividad de los sistemas de información críticos de la organización, los cuales generan alertas a los administradores ante la materialización de patrones anormales de comportamiento de dichos logs.
Se revisa por parte del auditor registro de logs relacionado con correos “bounced” remitidos desde el servidor de correo.

A.12.4.2 Protección de la información de registro
Solo los administradores de Sistemas pueden tener acceso a los registros de actividad.

A.12.4.3 Administrador y operador de registros
Se dispone de cuenta con privilegios para el Administrador de sistemas y las credenciales son conocidas por la responsable del Sistema de Gestión. Las tareas de administración de sistemas se realizan de manera operativa y habitual por parte del Administrador de Sistemas.
Los administradores, tienen dos cuentas de usuario, cuenta con usuario administrador, y cuenta como usuario estándar.

A.12.4.4 Sincronización del reloj
Los relojes de los sistemas se sincronizan con el reloj de tiempos de Ubuntu.

A.12.5 Control del software en explotación
A.12.5.1 Instalación de software en explotación
Las cuentas de usuario que utiliza el personal no son cuentas de administración locales, por lo que no se puede instalar software. En caso de que sea necesario instalar software en la infraestructura de la organización, se deberán utilizar las credenciales de Administrador de Sistemas.

A.12.6 Gestión de las vulnerabilidades técnicas
A.12.6.1 Gestión de vulnerabilidades técnicas
A.12.6.2 Restricciones en la instalación de software

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.12.7 Consideraciones sobre la Auditoría en los sistemas de información
A.12.7.1 Controles de auditoría de los sistemas de información

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.13. Seguridad de las comunicaciones

A.13.1 Gestión de la seguridad de las redes
A.13.1.1 Controles de red
A.13.1.2 Seguridad de los servicios de red
A.13.1.3 Segregación en redes

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.13.2 Intercambio de información
A.13.2.1 Políticas y procedimientos de intercambio de información
Se utiliza el correo electrónico con información de uso normalizado. Los clientes de la organización, cuando quiere notificar cualquier soporte lo realizan a través del portal de Tickets.
Se hace uso intensivo de internet y se aseguran las comunicaciones con el proveedor de servicios y la electrónica de red y comunicaciones.

A.13.2.2 Acuerdos de intercambio de información
Los acuerdos se determinan, principalmente, en los contratos.

A.13.2.3 Mensajería electrónica

Existe una protección del correo frente a amenazas, se emplea la protección de vadesecure a fin de evitar la salida de información clasificada fuera del dominio. Existen normas de uso y buenas prácticas del correo electrónico.
Se evidencia la modificación de links externos para asegurar por parte de vadesecure la seguridad de dichos accesos remotos.
La gestión del SPAM es realizada mediante servicios de SPAMExpert

A.13.2.4 Acuerdos de confidencialidad y no revelación
Se firman acuerdos de confidencialidad y protección de datos tanto para trabajadores como proveedores incluidos los docentes y los alumnos en la medida en que se requiere.
En la firma de los contratos de trabajo se incluye clausulado específico. Para los trabajadores se cuenta con Normativa de Seguridad de la información. Se evidencia su aceptación por parte de los trabajadores con la firma de la documentación. Evidencia contrato de confidencialidad muestreados: Miguel Angel Cedillo (11/02/2022), Jaime Sánchez Zamorano (18/07/2019), Alvaro Castro García (18/07/2019)
Con los proveedores se mantienen contratos con clausulado de confidencialidad y protección de datos y acuerdos de nivel de servicio en los casos en los que se requiere. Evidencia contrato de SLA con proveedor

A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información

A.14.1 Requisitos de seguridad en sistemas de información
A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información
A.14.1.2 Asegurar los servicios de aplicaciones en las redes públicas
A.14.1.3 Protección de las transacciones de servicios de aplicaciones

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.14.2 Seguridad en el desarrollo y en los procesos de soporte (respaldo)
A.14.2.1 Política de desarrollo de la seguridad
Este control no aplica

A.14.2.2 Procedimientos de control de cambios en sistemas
Se controlan mediante Zabbix, monitorizando en tiempo real los cambios que se detecten en el entorno de producción. Documentado en PS 02 Procedimiento de seguridad lógica.

A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
Solo los administradores de Sistemas pueden instalar/modificar la configuración de los equipos. Documentado en PS 03 Procedimiento de Control de accesos.

A.14.2.4 Restricciones sobre los cambios en los paquetes de software
Solo los administradores de Sistemas pueden instalar/modificar la configuración de los equipos. Documentado en PS 03 Procedimiento de Control de accesos.

A.14.2.5 Principios de ingeniería de sistemas seguros
La capa de seguridad se añade desde el diseño y por defecto en las distintas capas de arquitectura de la solución tecnológica
Documentado en PS 03 Procedimiento de Control de accesos.

A.14.2.6 Entorno de desarrollo seguro
No aplica por estar excluido.

A.14.2.7 Externalización del desarrollo de software
No aplica por estar excluido

A.14.2.8 Pruebas funcionales de seguridad del sistema
En caso de ser necesario su realización, se lleva a cabo por el Administrador de sistemas. Ante nuevas instalaciones y aplicaciones se prueban las aplicaciones con datos no reales. El entorno de las pruebas funcionales se intenta que sea el mismo que el del entorno de producción.

A.14.2.9 Pruebas de aceptación del sistema
Realizadas por el Administrador de sistemas de forma periódica. Principalmente, tras cambios importantes de nuevas aplicaciones y tecnología.

A.14.3 Datos de prueba (datos de entrada al equipo para el examen de la eficiencia del programa)
A.14.3.1 Protección de los datos de prueba (servidor de test)
No aplica por estar excluido.

A.15. Relación con proveedores

A.15.1 Seguridad en las relaciones con proveedores
A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores
A.15.1.2 Requisitos de seguridad en contratos con terceros
A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones

En la prestación de servicios por proveedores con relación en seguridad de la información se firman acuerdos de confidencialidad, protección de datos y de nivel de servicio, según corresponda.
Los proveedores de datacenter, tienen todos ellos certificados de seguridad. Walhalla y Kio, ENS nivel Alto, y Hetzner, ISO 27001.
En cuanto a comunicaciones, se trabaja con Vodafone, ENS Alto, y Orange, ENS Medio. Los acuerdos de nivel de servicio firmados con cada organización son los estándar establecidos por Vodafone en su red comercial (https://www.vodafone.es/c/statics/informaci%C3%B3n-de-calidad-de-servicio-vodafone-2023.pdf). Para Orange trimestalmente se dispone de acceso al informe público de SLAs en el que se consulta los SLAs establecidos (https://www.orange.es/static/pdf/2022T4_InformeCalidadOrange.pdf)
Se analiza en detalle al proveedor Walhalla como muestra de proveedores críticos de datacenter con SLA y acuerdo de confidencialidad firmado por las partes.

A.15.2 Gestión de la provisión de servicios del proveedor
A.15.2.1 Control y revisión de la provisión de servicios del proveedor
A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.16. Gestión de incidentes de seguridad de información

A.16.1 Gestión de incidentes de seguridad de la información y mejoras
A.16.1.1 Responsabilidades y procedimientos
A.16.1.2 Notificación de los eventos de seguridad de la información
A.16.1.3 Notificación de debilidades de seguridad
A.16.1.4 Evaluación y decisión sobre eventos de seguridad de la información
A.16.1.5 Respuesta a incidentes de seguridad de la información
A.16.1.6 Aprendizaje a partir de información de incidentes de seguridad de la información.
A.16.1.7 Recopilación de evidencia

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

A.17.1 Continuidad de la seguridad de la información
A.17.1.1 Planificación de la continuidad de la seguridad de la información
A.17.1.2 Implementar la continuidad de la seguridad de la información
A.17.1.3 Verificar, revisar y evaluar la continuidad de la seguridad de la información

Se ha revisado el documento: PS 05 Anexo I Plan de Continuidad v1. 1.1 20/02/2023 Revisión del documento. Se comprueba que se tienen bien documentadas la planificación de las pruebas de continuidad en el documento: FO.PS.05-03 Plan de Pruebas de Continuidad.

En el plan de continuidad, se encuentran definidos los siguientes escenarios de continuidad:
6.1 Fallo del proveedor de hosting
6.2 Fallo del proveedor de Cloud
6.3 Fallo en la centralita telefónica
6.4 Pérdida o fallo de integridad de una base de datos

Mejora 3: Definir más escenarios de continuidad. Ejemplos: Desastre en las oficinas; Posible escenario de caída del servicio de ofimática, y del servicio de correo electrónico.

A.17.2 Redundancias
A.17.2.1 Disponibilidad de los recursos de tratamiento de la información.

La revisión de estos controles no se encuentra planificada para esta auditoría.

A.18. Cumplimiento

A.18.1 Cumplimiento de los requisitos legales y contractuales
A.18.1.1 Identificación de la normativa aplicable y los requisitos contractuales
Los requisitos legales y normativos de las actividades de QUER Systems y en materia de la seguridad de la información se encuentran bien dcumentos.
Entre otras normativas, se evidencia la aplicación en las siguientes materias:
- Protección de datos: Ley 3/2018 y RGPD 2016/679.
- Propiedad intelectual: RDL 1/1996.
- Servicios de seguridad de la información y servicios electrónicos: Ley 34/2002 LSSICE y Ley 6/2020.

A.18.1.2 Derechos de propiedad intelectual
En relación a la propiedad intelectual y el uso de software se controla el licenciamiento de productos.
Se tiende en la organización a la utilización de software gratuito, como por ejemplo paquetes ofimáticos gratuitos, antivirus ClamAV (software también gratuito), tanto para los servidores, como para los PCs de usuario.

A.18.1.3 Protección de registros
La custodia de la información en soporte papel se realiza por parte de RR.HH. y Administración y se protege en los armarios de los despachos.
Las copias de seguridad aseguran, entre otras, la pérdida y destrucción de los datos y la información.

A.18.1.4 Protección y privacidad de la información de carácter personal

Se cumple la normativa en materia de protección de datos con los trabajadores en los contratos laborales. Durante la auditoría se ha revisado documentación relativa a la protección de datos de los clientes, proveedores y personal de la organización.

Se ha implantado un Sistema de Gestión de la Privacidad que contempla el cumplimiento de todos los aspectos relacionados con el tratamiento de datos de carácter personal. Se dispone de contrato de asesoramiento en materia de Protección de Datos con la organización A3SIDES para la implantación y mantenimiento.
Se evidencia existencia de RAT, Política de Privacidad (web), Contratos Responsable-Encargado con los proveedores y Cláusulas legales a incorporar a los diferentes documentos gestionados por la organización.
Evidencias: Contratos de Encargados (A3SIDES, Gesprefor, Wallhalla), Contratos de confidencialidad muestreados: Miguel Angel Cedillo, Jaime Sánchez Zamorano, Alvaro Castro García, Walter Urbiña.

A.18.1.5 Reglamento de controles criptográficos

Se cumple el requisito funcional del certificado de la página web. Se dispone de certificado SSL R3 válido emitido por Let´s encrypt, que fue renovado el pasado 14 de Mayo del 2023.

En cuanto al portal de Tickets, está proporcionado por el proveedor Altasian.

Se comprueba mediante el aplicativo Security Headers que las cabeceras del portal de tickets (https://quersystem.atlassian.net/servicedesk/customer/portal/15/user/login?destination=portal%2F15), están correctamente configuradas, obteniéndose una A

A.18.2 Revisión de la seguridad de la información
A.18.2.1 Revisión independiente de la seguridad de la información
A.18.2.2 Cumplimiento de las políticas y normas de seguridad
A.18.2.3 Revisión del cumplimiento técnico

La revisión de estos controles no se encuentra planificada para esta auditoría.

(5) EVALUACIÓN DEL CUMPLIMIENTO LEGAL AMBIENTAL Y/O DE SEGURIDAD Y SALUD LABORAL. *Hacer una valoración sobre la conformidad y la eficacia del SGA de la organización y si tiene la capacidad para detectar los requisitos legales que le aplican, para evaluar su cumplimiento y para cumplirlos.*

¿Tiene capacidad para identificar requisitos legales de aplicación? N/A

¿Tiene capacidad para cumplir dichos requisitos? N/A
(Es caso negativo debe identificarse desviaciones al respecto, en el apartado correspondiente)

¿Existe una planificación de actuación para conseguir cumplimiento? N.A
(En caso de existir tiene asignados recursos, presupuesto y esta priorizado)

(6) OTRAS CONSIDERACIONES.

Se ha evidenciado durante toda la auditoria la buena disposición por parte de la organización a la hora de informar y mostrar y poner a disposición del equipo auditor toda la información que se le ha ido solicitando para la realización de la misma.

Se hace especial constancia de la implicación y voluntad de mejora por parte de las personas que han participado en la auditoría, destacando el conocimiento en la materia y la disponibilidad y atenciones para la realización de la misma.

Se agradece a la empresa las facilidades dadas para la realización de esta auditoría.

(7) COMENTARIOS Y OPORTUNIDADES DE MEJORA.

COMENTARIOS/OBSERVACIONES:

Ref. DESV	DESCRIPCIÓN DE LOS COMENTARIOS
COM 1	Modificar el punto 4.4.2.- 4.4.2. Roles, para incluir los miembros correctos, de cara a evitar discrepancias se recomienda disponer de un único repositorio donde se incluyan los diferentes cargos.
COM 2	Incluir en los indicadores los correspondientes a la eficiencia en horas y presupuesto del PACS de resolución de la certificación en el ENS.
COM 3	Como viene recogida en la no conformidad 6 identificada en la auditoría del ENS se recomienda tanto para los nuevos como para los antiguos empleados, la firma de un nuevo documento de confidencialidad, donde se precise un periodo de tiempo de varios años de mantener la confidencialidad de la información, después de haber abandonado la empresa.

Nota: Los comentarios u observaciones si no se tienen en futuras auditorías, son susceptibles de convertirse en desviaciones.

MEJORAS:

Ref. DESV	DESCRIPCIÓN DE LAS MEJORAS
Mejora 1	Profundizar en el DAFO (bajarlo in poco de nivel), orientándolo mucho más a Seguridad de la Información. Dado que se utiliza un cuestionario para realizar el DAFO, se recomienda incluir más preguntas orientadas a la Seguridad de la información, privacidad y cloud.
Mejora 2	Se recomienda, para facilitar la evolución entre un año y el siguiente de los Riesgos y de los Planes de Tratamiento de las correspondientes salvaguardas, pasar el análisis de Riesgos y sobre todo el PTR de Word a documentos de excel, lo que facilita la comparativa entre un año y el siguiente. De esta forma también se está más en línea con lo exigido por el ENS en relación con este control.
Mejora 3	Definir más escenarios de continuidad. Ejemplos: Desastre en las oficinas, Posible escenario de caída del servicio de ofimática, y del servicio de correo electrónico.
Mejora 4	La longitud mínima de las contraseñas admitida es de 8 caracteres, se recomienda subir la longitud de la contraseña mínimo a 12 caracteres. Actualmente una contraseña de tan sólo 8 caracteres se considera insegura.

RECOMENDACIÓN DEL EQUIPO AUDITOR

Marcar lo que proceda:

AUDITORÍA DE CERTIFICACIÓN

☐ Conceder la certificación para: ☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☒SSI ☐ Otra

☐ Conceder la certificación **(si surgen no conformidades o desviaciones)** condicionada a recibir de la empresa un plan satisfactorio de acciones correctivas y las evidencias que demuestren la eficacia de su implantación **en la fecha indicada en el Anexo_Impreso AU-02-03**[2] para: ☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra

Nota importante:
Transcurrido el plazo de 6 meses sin que se hayan cerrado las no conformidades, la auditoría no tendrá validez a los efectos de la certificación, y deberá iniciarse el proceso con una nueva auditoría de certificación.

Auditoría extraordinaria
☐ No
☐ SI, en el plazo de X meses para: ☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra

AUDITORÍA DE SEGUIMIENTO/RECERTIFICACIÓN

☒ Mantener/Renovar la certificación para: ☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra

☐ Mantener o Renovar la certificación **(si surgen únicamente desviaciones)** condicionada a recibir un plan de acciones correctivas **en la fecha indicada en Anexo_Impreso AU-02-03**[2]. En el caso de no recibir el plan de acciones correctivas en el plazo establecido, se suspenderá temporalmente la certificación hasta su recepción para:
☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra

☐ Suspender temporalmente la certificación **(si surgen no conformidades)** si **en la fecha indicada en Anexo_Impreso AU-02-03**[2] desde la auditoría no se ha recibido el plan de acciones correctivas y las evidencias que demuestren la eficacia de su implantación para: ☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra

Auditoría extraordinaria
☐ No
☐ SI, en el plazo de X meses para: ☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra

[2] Anexo Impreso AU-02-03, es el documento que se entrega el día de la auditoría donde aparecen las NC / DESV

EVALUACIÓN DEL PLAN DE ACCIONES CORRECTIVAS - EVIDENCIAS (si se envían)

NO CONFORMIDADES:

No se han hallado

DESVIACIONES:

No se han hallado

Ref. DESV	DESCRIPCIÓN DE LAS DESVIACIONES	NORMA Punto

** Debido al carácter puntual y muestral de la auditoría, se recuerda a la empresa que la resolución de las desviaciones no debe limitarse única y exclusivamente a la resolución de los ejemplos indicados en las mismas, sino que se debe realizar una investigación a fin de determinar el alcance de estas desviaciones y establecer acciones para resolverlas y que no vuelvan a reproducirse.*

RECOMENDACIÓN FINAL

AUDITORÍA

☐ DENEGAR LA CERTIFICACIÓN
☐ CONCEDER LA CERTIFICACIÓN
☒ MANTENER LA CERTIFICACIÓN
☐ SUSPENDER LA CERTIFICACIÓN
☐ CANCELAR LA CERTIFICACIÓN
CON:
☐ Auditoría ordinaria para: ☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra
☐ Auditoría extraordinaria en el plazo de X meses para: ☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra

Auditor Jefe:
Fecha:

REVISIÓN TÉCNICA (por IVAC)

☐ Revisión auditoría en remoto (si procede)

☐ DENEGAR LA CERTIFICACIÓN
☐ CONCEDER LA CERTIFICACIÓN
☐ MANTENER LA CERTIFICACIÓN
☐ SUSPENDER LA CERTIFICACIÓN
☐ CANCELAR LA CERTIFICACIÓN
CON:
☐ Auditoría ordinaria para: ☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra
☐ Auditoría extraordinaria en el plazo de X meses para: ☐SGC ☐SGA ☐ SGCTT ☐SGIDi ☐SST ☐SSI ☐ Otra

Revisor:
Fecha:

SGC calidad	SGA medio ambiente	SGCTT tacógrafos	SGIDi investigación	SST seguridad	SSI información

EVALUACIÓN DE LA AUDITORÍA POR PARTE DEL EQUIPO AUDITOR

Tiempo estimado	☒ Suficiente	☐ Insuficiente (1)	☐ Excesivo(2)
Alcance de la auditoría	☒ Adecuado	☐ Inadecuado (3)	
Objetivo de la auditoria	☒ Adecuado	☐ Inadecuado (3)	
Documentos IVAC	☒ Suficientes	☐ Insuficientes	

(1) Indicar que aspectos no han quedado adecuadamente evaluados, cuanto tiempo ha faltado y por qué
(2) Indicar cuanto tiempo ha sobrado y por qué
(3) Indicar que aspectos no han sido considerados

Otras consideraciones

AUDITORIAS EN REMOTO

Cumplimentar en caso de que en el desarrollo de la auditoria se utilicen alguna de las técnicas para auditorias en remoto.

No se ha desarrollado ni total ni parcialmente la auditoría en remoto.

Plataforma IT utilizada (Teams, Zooms, etc):

TIC usados:

- Revisión documental (no en tiempo real): ☒ SÍ ☐ NO Comentarios:
- Video: (para visita a las instalaciones) ☐ SÍ ☒ NO Comentarios:
- Grabaciones: ☐ SÍ ☒ NO Comentarios:
- Captura de pantallas: ☒ SÍ ☐ NO Comentarios:
- Intercambio de fotografías: ☒ SÍ ☐ NO Comentarios:
- Otros:

- ¿El uso de estas TICs ha permitido alcanzar los objetivos previstos de esta auditoría? SI
- ¿Se consideran adecuados los riesgos asumidos para el uso de las TICs? SI