Auditoría ISO 27001, VLS Group

Fecha del Informe: 6 de marzo de 2023
Cliente: VLS Group
Auditor: Capgemini Málaga

1. Introducción

VLS Group es un proveedor europeo líder en soluciones logísticas avanzadas para la industria química y sectores relacionados. Este informe detalla los hallazgos de la auditoría de seguridad de la información realizada conforme a los requisitos de la norma ISO 27001:2022, que establece un marco para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

El propósito de la auditoría es evaluar la eficacia de los controles implementados, identificar posibles riesgos de seguridad y ofrecer recomendaciones para mitigar esos riesgos.

---

2. Objetivo de la Auditoría

El objetivo de esta auditoría es verificar el cumplimiento del SGSI de VLS Group con los requisitos de la norma ISO 27001 y asegurar que los controles de seguridad de la información sean adecuados para proteger la confidencialidad, integridad y disponibilidad de la información sensible, particularmente relacionada con la gestión de productos químicos, logística y transporte.

---

3. Alcance de la Auditoría

La auditoría abarcó todas las áreas críticas del negocio de VLS Group, incluyendo:

- **Infraestructura TI:** Servidores, bases de datos, redes, y sistemas de gestión de productos químicos.
- **Operaciones:** Procesos de manipulación y transporte de productos químicos.
- **Usuarios y empleados:** Políticas de acceso y formación en seguridad.
- **Proveedores externos:** Relaciones con terceros y proveedores de servicios logísticos.
- **Instalaciones físicas:** Almacenes y centros de distribución.

4. Metodología

La auditoría se realizó utilizando una combinación de técnicas cualitativas y cuantitativas, tales como:

- Entrevistas con personal clave (TI, operaciones y gerencia).
- Revisión de políticas y procedimientos internos.
- Evaluaciones técnicas de seguridad (pruebas de penetración, análisis de vulnerabilidades).

- Revisión de la documentación del SGSI.
- Análisis de registros y auditorías anteriores.

5. Evaluación del Sistema de Gestión de Seguridad de la Información (SGSI)

El SGSI de VLS Group fue evaluado en base a los siguientes componentes clave:

1. **Política de Seguridad de la Información:** Se revisaron las políticas para garantizar que están actualizadas, alineadas con la normativa ISO 27001 y correctamente comunicadas al personal.
2. **Liderazgo y Compromiso:** El compromiso de la alta dirección en el mantenimiento del SGSI se consideró adecuado, con roles y responsabilidades claramente definidos.
3. **Gestión de Riesgos:** Se evaluó la metodología de análisis de riesgos implementada y la efectividad de los controles de mitigación.

---

6. Revisión del Cumplimiento con la ISO 27001

Se revisaron los controles establecidos en los Anexos A de la ISO 27001. A continuación se detallan los hallazgos por cada dominio.

---

7. Resultados de la Auditoría

A. Política de Seguridad de la Información

Hallazgo:

- Existe una política de seguridad de la información, pero no ha sido actualizada en los últimos 12 meses.
- No está claro si todos los empleados han sido informados adecuadamente sobre los cambios más recientes.

Recomendación:

- Actualizar la política anualmente y asegurarse de que se realicen capacitaciones obligatorias para todo el personal.

B. Organización de la Seguridad de la Información

Hallazgo:

- Se observó que existe un equipo dedicado a la gestión de la seguridad de la información, pero la comunicación entre departamentos no es eficaz.

- No se ha formalizado un Comité de Seguridad de la Información que involucre a todas las áreas clave.

Recomendación:

- Establecer un Comité de Seguridad con representantes de TI, operaciones y logística para fomentar una mejor coordinación y gestión de riesgos.

C. Gestión de Activos

Hallazgo:

- Existe un inventario de activos de TI, pero no incluye todos los dispositivos móviles utilizados por los empleados en campo, lo que representa un riesgo.
- No se están realizando auditorías periódicas de los activos críticos.

Recomendación:

- Completar el inventario con todos los dispositivos móviles y realizar auditorías trimestrales de los activos críticos.

D. Seguridad en Recursos Humanos

Hallazgo:

- Se han implementado controles para la contratación y finalización de empleados, pero no se realizan verificaciones exhaustivas de antecedentes para contratistas.

Recomendación:

- Implementar procedimientos de verificación de antecedentes para todos los contratistas y personal temporal.

E. Control de Accesos

Hallazgo:

- Las políticas de control de acceso son sólidas, pero se detectaron inconsistencias en la implementación de controles de acceso basados en roles (RBAC) en ciertos sistemas de logística.

Recomendación:

- Revisar los roles y permisos de los usuarios y aplicar el principio de mínimos privilegios en todos los sistemas críticos.

F. Criptografía

Hallazgo:

- Se utiliza criptografía fuerte (AES-256) para la protección de datos en tránsito y en reposo. Sin embargo, no se está realizando una gestión adecuada de las claves de cifrado.

Recomendación:

- Implementar un sistema de gestión de claves (KMS) centralizado y llevar un registro de auditoría de todas las actividades relacionadas con las claves de cifrado.

G. Seguridad Física y Ambiental

Hallazgo:

- Las instalaciones clave cuentan con sistemas de control de acceso físico y videovigilancia, pero se detectaron áreas críticas sin control de acceso biométrico.

Recomendación:

- Implementar sistemas de acceso biométrico en todos los almacenes donde se manipulan productos químicos peligrosos.

H. Seguridad en las Operaciones

Hallazgo:

- Los procesos de seguridad en las operaciones diarias son adecuados. Sin embargo, se identificó que no hay un plan formalizado de gestión de parches.

Recomendación:

- Formalizar y automatizar el proceso de gestión de parches para garantizar la actualización oportuna de todos los sistemas.

I. Seguridad en las Comunicaciones

Hallazgo:

- Las comunicaciones internas y externas están protegidas, pero no se realiza una monitorización continua de las comunicaciones sensibles.

Recomendación:

- Implementar soluciones de monitoreo continuo de redes para identificar actividades sospechosas o no autorizadas.

J. Gestión de Incidentes de Seguridad de la Información

Hallazgo:

- Existe un proceso de gestión de incidentes, pero no se han realizado simulacros de incidentes en los últimos 18 meses.

Recomendación:

- Realizar simulacros de respuesta a incidentes al menos una vez al año para mejorar la capacidad de respuesta ante eventos reales.

---

8. Recomendaciones Generales

- **Fortalecer la formación en seguridad**: Realizar entrenamientos periódicos de concienciación de seguridad para todo el personal.
- **Automatizar procesos de auditoría y monitoreo**: Implementar herramientas SIEM para el monitoreo centralizado de la infraestructura.
- **Revisar proveedores externos**: Establecer acuerdos de nivel de servicio (SLA) claros en términos de seguridad de la información con todos los proveedores.

---

9. Conclusiones

En general, el SGSI de VLS Group se encuentra bien estructurado y cumple con muchos de los requisitos de la norma ISO 27001. Sin embargo, **se identificaron áreas clave que requieren atención, como la gestión de activos, control de accesos y respuesta a incidentes.** La implementación de las recomendaciones proporcionadas mejorará la postura de seguridad de la organización y facilitará el cumplimiento continuo con la norma.

Capgemini Málaga
C. Severo Ochoa, 61, Campanillas, 29590 Málaga