TECNICATURA UNIVERSITARIA EN CIBERSEGURIDAD

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (MARCOS NORMATIVOS)

Unidad I – Trabajo práctico N°3

Profesor: Lic. Juan Pablo Villalba

Alumno: Balbuena Atar Dante Gabriel

Tucumán, Tafí Viejo – septiembre 2024

Contenido

1. Introducción

EcoTech S.A. es una empresa mediana que se especializa en la producción de productos ecológicos, incluyendo envases biodegradables y productos de limpieza sostenibles. La empresa ha experimentado un crecimiento significativo en los últimos años, impulsado por la creciente demanda de productos respetuosos con el medio ambiente. Con la digitalización de sus operaciones, EcoTech ha aumentado su dependencia de las tecnologías de la información, lo que ha llevado a la dirección a considerar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO 27001.

Al utilizar un enfoque práctico para la auditoría y gestión de la seguridad de la información en EcoTech S.A. nos permite no solo cumplir con los requisitos normativos sino también asegurar que la gestión de la seguridad de la información se integre de manera efectiva en la misión y visión de EcoTech S.A., contribuyendo al crecimiento sostenible de la empresa

2. Desarrollo

1. Modelo PDCA:

PLAN

1. Identificación de Información Sensible
2. Definición de Roles y Permisos
3. Desarrollo de la Política de Acceso
4. Documentación del Proceso

DO

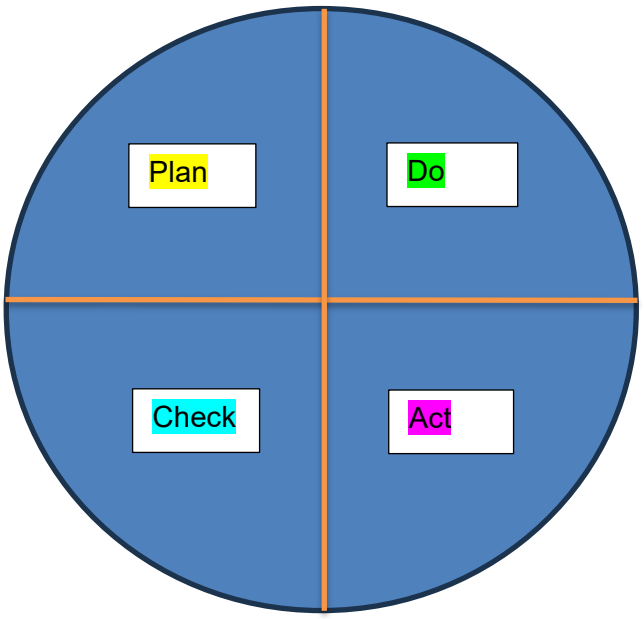
1. Implementación de Controles Basados en Roles
2. Capacitación del Personal.
3. Despliegue de Herramientas Tecnológicas

CHECK

1. Monitoreo del Acceso
2. Revisión de Incidencias
3. Auditoría Interna.

ACT

1. Corrección de Desviaciones.
2. Actualización de Políticas.
3. Mejora Continua.



2. Programa de Auditoría:

A. Objetivos de la auditoría y criterios de evaluación:

Objetivos: Verificar que se cumpla el SGSI en Eco Tech S.A. en relación con la norma ISO 27001, tanto en los aspectos de la efectividad de los controles, las políticas y procedimientos deben estar alineados con la seguridad de la inf. y revisar el cumplimiento de las normativas ambientales y de protección de datos.

Criterios: en referencia a las cláusulas 4 a 10 de ISO 27001 (Contexto de la organización, Liderazgo y compromiso, Planificación, Apoyo y recursos, Operación, Evaluación del desempeño, Mejora continua.

B. Cronograma de auditorías internas y externas, incluyendo revisiones de cumplimiento con normativas ambientales y de protección de datos:

Auditorías internas		Auditorías Externas	
Frecuencia	Anual o semestral	Frecuencia	Antes de la certificación y cada tres años para la recertificación.
Alcance	Revisar los controles internos, procedimientos de seguridad de la	Alcance	Revisión completa del SGSI por parte de un auditor externo autorizado para la

	información y políticas de acceso, con un enfoque específico en los controles basados en roles		certificación ISO 27001
Áreas clave	Gestión de accesos, Protección de datos sensibles, Cumplimiento con las normativas aplicables, Gestión de incidentes de seguridad	Áreas clave	Verificación del cumplimiento con todas las cláusulas de la norma ISO 27001, Evaluación del tratamiento de riesgos y la implementación de los controles recomendados

Revisión de Cumplimiento Normativo	
Normativas Ambientales	Para asegurar que los procesos digitales y físicos relacionados con productos sostenibles cumplen con regulaciones locales o internacionales.
Normativa de Protección de Datos	Verificar el cumplimiento con leyes como el RGPD en caso de que EcoTech maneje datos de ciudadanos de la Unión Europea o regulaciones locales equivalentes.

3. Checklist de Entrevista:
    1. ¿De qué manera se asegura que el Sistema de Gestión de Seguridad de la Información (SGSI) esté en sintonía con los objetivos estratégicos y operativos de EcoTech S.A.?
    2. ¿Cómo demuestra la alta dirección su compromiso con la seguridad de la información y la implementación del SGSI?
    3. ¿Está establecida una política de seguridad de la información en EcoTech S.A., y cómo se asegura su comunicación efectiva a empleados y otras partes interesadas?
    4. ¿Qué proceso se sigue para gestionar los riesgos de seguridad de la información en el SGSI y qué criterios se utilizan para evaluarlos?
    5. ¿Qué tipos de controles se han puesto en marcha para reducir los riesgos identificados y cómo se seleccionaron estos controles?
    6. ¿Cómo garantiza la empresa que sus empleados reciben la formación adecuada en gestión de seguridad de la información?
    7. ¿Qué recursos (en términos de personal, tecnología y presupuesto) se han asignado para el funcionamiento y la mejora continua del SGSI?
    8. ¿Qué procedimientos existen para responder a incidentes de seguridad y cómo se manejan las situaciones de no conformidad?
    9. ¿Cómo se lleva a cabo el seguimiento, la medición y el análisis de la efectividad del SGSI, y con qué frecuencia se revisa?
    10. ¿Qué mecanismos tiene la empresa para identificar oportunidades de mejora dentro del SGSI y para abordar las no conformidades?

4. Política del SGSI:

    1. Lo que observo de la política brindada por EcoTech S.A. en un contexto real sería considerada como pobre de contenido pero en un contexto lo cual se intenta ser lo más resumido posible esto es factible, sin embargo mencionare algunos aspectos fuertes y a mejorar. desde lo positivo empezamos que los altos mandos están comprometidos, menciona la protección de la información con el cumplimiento de leyes y regulaciones y al mismo tiempo resalta el alineamiento con los objetivos de la empresa que sería el cuidado del medio ambiente. Mejoraría la definición en los

activos de información a cubrir y cuanto abarca el SGSI y la designación de responsabilidades para cada área o empleado.

5. Plan de Auditoría:

Sección	Descripción
Objetivo	Evaluar conformidad con ISO 27001 y eficacia del SGSI.
Alcance	Todo el SGSI: políticas, gestión de riesgos, respuesta a incidentes.
Criterios	Cumplimiento con ISO 27001, políticas internas, requisitos legales.
Plan	1. Preparación: Revisión de documentación y entrevistas. 2. Evaluación de la Política: Verificación de existencia, adecuación y comunicación. 3. Gestión de Riesgos: Revisión de identificación, evaluación y controles de riesgos. 4. Capacitación: Confirmación de formación en seguridad de la información. 5. Recursos y Responsabilidades: Evaluación de recursos asignados y claridad de responsabilidades. 6. Respuesta a Incidentes: Revisión de procedimientos y efectividad. 7. Seguimiento y Mejora: Evaluación de métodos de seguimiento y procesos de mejora continua.
Cronograma	-Preparación: [Fecha] -Evaluación en Sitio: [Fecha] -Informe Preliminar: [Fecha] - Informe Final: [Fecha]
Recursos	-Auditor interno/externo - Acceso a documentación y personal clave.
Comunicación	Informe a la alta dirección, recomendaciones y plan de seguimiento.

6. Reunión de Inicio:

1. Primero reuniría a los participantes (auditor jefe, equipo de auditoría, representantes de EcoTech S.A.) luego de definiria una agenda con objetivos y tiempo de duración y una documentación clara. iniciaría con una introducción (bienvenida, el propósito y la importancia de la auditoria), explicaría el cronograma y la metodología, los roles y responsabilidades, como seria la comunicación, como evaluamos y que expectativas esperamos, aclarar dudas y responderlas cerrando con una conclusión.

7. Evaluación de Riesgos:

El sistema de evaluación de riesgos es muy simplificado ya que está configurado con Excel y este no tiene tantas funcionalidades avanzadas, se relaciona con la cláusula 6.1.2 Evaluación y tratamiento de riesgos de seguridad de la información.

carece de formalidad que genera desconfianza se relaciona con la cláusula 6.1.2 - Evaluación y tratamiento de riesgos de seguridad de la información.

Los activos no están clasificados según su importancia crítica y por lo tanto no se puede asignarle un nivel de riesgo, se relaciona con la cláusula 8.1 - Identificación y evaluación de activos.

No indica que se lleve a cabo actualizaciones y mantenimiento, se relaciona con la cláusula 9.2 - Monitoreo, revisión y evaluación.

La documentación debe ser más detallada, se relaciona con la cláusula 7.5 - Control de la documentación.

8. Pruebas de Seguridad:

A. Determinación de No Conformidad

Situación: No se han realizado pruebas de restauración de datos en los últimos seis meses.

Clasificación:

Tipo: No Conformidad Mayor

Justificación: La falta de pruebas de restauración de datos puede comprometer la capacidad de recuperación en caso de pérdida de datos, afectando la integridad y disponibilidad de la información crítica.

Requisito ISO 27001 Relacionado:

Cláusula 9.1.2: Se requiere monitoreo y evaluación continua de la eficacia de los controles.

B. Selección y Clasificación de No Conformidades

1. No Conformidad: Falta de Documentación de Pruebas de Restauración

   Descripción: La documentación de las pruebas de restauración es incompleta o inexistente.

   Clasificación: No Conformidad Mayor

   Justificación: La documentación adecuada es esencial para evidenciar que las pruebas se han realizado correctamente.

   Requisito ISO 27001 Relacionado: Cláusula 7.5: Control de la documentación.

2. No Conformidad: Ausencia de Cronograma para Pruebas de Restauración

   Descripción: No hay un cronograma establecido para realizar pruebas periódicas de restauración.

   Clasificación: No Conformidad Menor

   Justificación: La planificación regular de las pruebas es crucial para asegurar su realización oportuna y efectiva.

   Requisito ISO 27001 Relacionado: Cláusula 8.2: Evaluación de riesgos y gestión de controles.

9. Informe de Auditoría:

Portada: Informe de Auditoría de Certificación ISO 27001 para EcoTech S.A. Fecha: [Fecha]. Auditor Jefe: [Nombre].

Índice:

Introducción, Alcance y Objetivos, Metodología, Resultados, No Conformidades, Conclusiones y Recomendaciones, Anexos

Introducción: El informe resume los hallazgos de la auditoría realizada para evaluar el cumplimiento de EcoTech S.A. con la norma ISO 27001.

Alcance y Objetivos: Se auditó el SGSI de EcoTech S.A. para verificar su conformidad con la norma ISO 27001 y evaluar la eficacia de los controles implementados.

Metodología: La auditoría incluyó entrevistas, revisión de documentos y pruebas, realizada en [fechas].

Resultados: Se observó una falta de pruebas de restauración de datos y deficiencias en la documentación y planificación de dichas pruebas.

No Conformidades:

Falta de Pruebas de Restauración de Datos: No se realizaron pruebas en los últimos seis meses. Clasificación: Mayor. Requisito: Cláusula 9.1.2.

Falta de Documentación de Pruebas: La documentación es incompleta o inexistente. Clasificación: Mayor. Requisito: Cláusula 7.5.

Ausencia de Cronograma: No hay un cronograma para pruebas periódicas. Clasificación: Menor. Requisito: Cláusula 8.2.

Conclusiones y Recomendaciones: Las no conformidades afectan la capacidad de recuperación y la documentación del SGSI. Se recomienda implementar un plan de acción para corregir las deficiencias.

10. La reunión de cierre debe incluir a los participantes clave como el auditor jefe y representantes de EcoTech S.A., con el objetivo de presentar los hallazgos, discutir las no conformidades detectadas, y establecer un plan de acción. Se debe iniciar con una introducción y un resumen de los hallazgos generales, seguido por la presentación detallada de cada no conformidad, incluyendo la falta de pruebas de restauración de datos, la falta de documentación, y la ausencia de cronograma. La discusión debe centrarse en el impacto de estas no conformidades y acordar las acciones correctivas necesarias, incluyendo plazos y responsables. Finalmente, se debe abordar los próximos pasos, responder preguntas, y cerrar la reunión con un resumen de acuerdos y agradecimientos.

3. Conclusiones

La auditoría de EcoTech S.A. destacó áreas clave de mejora en su Sistema de Gestión de Seguridad de la

Información (SGSI), particularmente en la realización de pruebas de restauración de datos, documentación y planificación. Las no conformidades identificadas requieren acciones correctivas específicas y oportunas para asegurar el cumplimiento con la norma ISO 27001. Se acordaron medidas concretas y plazos para resolver estos problemas, con un seguimiento planificado para verificar la eficacia de las acciones implementadas. La empresa ha demostrado compromiso con la mejora continua y con la seguridad de la información.

4. Referencias:

ISO. (n.d.). *ISO/IEC 27001 Information Security Management*. International Organization for Standardization. Retrieved from https://www.iso.org/isoiec-27001-information-security.html
IT Governance. (n.d.). *ISO 27001 Overview*. Retrieved from https://www.itgovernance.co.uk/iso27001
MindTools. (n.d.). *PDCA Cycle*. Retrieved from https://www.mindtools.com/pages/article/newLDR_86.htm
ASQ. (n.d.). *PDCA Model*. Retrieved from https://asq.org/quality-resources/pdca-cycle
ISO. (n.d.). *ISO 9001:2015 - Quality Management Systems*. International Organization for Standardization. Retrieved from https://www.iso.org/standard/62085.html
Smartsheet. (n.d.). *Audit Program Examples*. Retrieved from https://www.smartsheet.com/creating-audit-program
The Auditor Exchange. (n.d.). *ISO 27001 Audit Questions*. Retrieved from https://www.theauditor.exchange/iso-27001-audit-questions/
SANS. (n.d.). *Developing Information Security Policies*. Retrieved from https://www.sans.org/white-papers/38577/
Project Management Docs. (n.d.). *Audit Plan Template*. Retrieved from https://www.projectmanagementdocs.com/template/project-planning/audit-plan/
Project Management Docs. (n.d.). *Audit Plan Template*. Retrieved from https://www.projectmanagementdocs.com/template/project-planning/audit-plan/
IT Governance. (n.d.). *Risk Assessment ISO 27001*. Retrieved from https://www.itgovernance.co.uk/risk-assessment
National Institute of Standards and Technology (NIST). (2010). *Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev. 1)*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final
ISO. (n.d.). *ISO 9001 Quality Management*. International Organization for Standardization. Retrieved from https://www.iso.org/iso-9001-quality-management.html
Quality Assurance Solutions. (n.d.). *Audit Closing Meeting*. Retrieved from https://www.qasolutions.net/audit-closing-meeting/

Este documento sigue las normas de citación y referencias de la *Publication Manual of the American Psychological Association* (7ª ed.).