Centro de Especializaciones Noeder

Diploma de Especialización Internacional

IMPLEMENTADOR Y AUDITOR SEGURIDAD DE LA INFORMACIÓN - ISO 27001 Y CONTINUIDAD DEL NEGOCIO - ISO 22301

CLASE 06

FORMACIÓN DE AUDITOR INTERNO EN LAS NORMAS ISO 27001 E ISO 22301 – PARTE II

Mg. Ing. Julio Pereyra Rosales

1. PRINCIPIOS DE AUDITORÍA

Integridad

- Realizar la auditoría de forma ética, con honestidad y responsabilidad.
- Sólo realizar actividades de auditoría si es competente para hacerlo.
- Realizar la auditoría de manera imparcial.
- Ser sensible a cualquier influencia que pueda ejercer sobre su juicio mientras lleva a cabo una auditoría.

Presentación Razonable

- Los hallazgos de la auditoría, las conclusiones de auditoría y los informes de auditoría deberían reflejar de manera veraz y precisa las actividades de auditoría.
- La comunicación es veraz, precisa, objetiva, oportuna, clara y completa.

1. PRINCIPIOS DE AUDITORÍA

Los auditores deben tener el debido cuidado de acuerdo con la importancia de la tarea que realizan y la confianza depositada en ellos por el cliente de auditoría y otras partes interesadas.

Los auditores ejercen discreción en el uso y la protección de la información adquirida en el desempeño de sus funciones.

1. PRINCIPIOS DE AUDITORÍA

Independencia

Los auditores debe ser independiente de la actividad auditada siempre que sea posible y, en todos los casos, deberían actuar de forma tal que no estén sujetos a prejuicios ni a conflictos de intereses.

Enfoque en el Riesgo

El enfoque basado en el riesgo influye sustancialmente en la planificación, conducción y presentación de informes de las auditorías para garantizar que las auditorías se centren en asuntos que son importantes para el cliente de auditoría y para lograr los objetivos del programa de auditoría.

1. PRINCIPIOS DE AUDITORÍA

Enfoque basado en evidencia.

- La evidencia de auditoría es verificable.
- En general, se basa en muestras de la información disponible, ya que una auditoría se lleva a cabo durante un tiempo finito y con recursos limitados.
- Se debería aplicar un uso apropiado del muestreo, ya que está estrechamente relacionado con la confianza que se puede depositar en las conclusiones de la auditoría.

2. GESTIÓN DEL RIESGO

MATRIZ DE RIESGOS

	ELABORADO POR:	REVISADO POR:	APROBADO POR:	FECHA ACTUALIZACIÓN	PROCESO
	Auditor	Auditor Lider	Auditor Lider	1/05/24	AUDITORÍA INTERNA

ACTIVIDADES	DESCRIPCIÓN DEL RIESGO			CONTROL ACTUAL	VALORACION			NIVEL DE RIESGO	ACCIONES POR IMPLEMENTAR	RE - VALORACION			NIVEL DE RIESGO
	FUENTE DE RIESGO	CONSECUENCIA(S) DEL RIESGO	CAUSA (S) DE LA FUENTE DE RIESGO		G	O	D	(G x O x D)		G	O	D	(G x O x D)
Auditoría Interna	Auditor no competente	El proceso de auditoria no se cumplirá de manera adecuada	Auditor no capacitado	Plan de capacitación , seguimiento de eficacia de los entrenamientos	5	3	3	45	1. Establecer mecanismos de verificación con cada auditado de proceso.	5	2	2	20
	No se cumpla con el programa de auditoria.	No se tiene los informes de auditoria a tiempo	Demora en los procesos Auditados.	Se debe revisar y ajustar el plan de auditoria	3	2	1	6	No aplicable				0
	Demora en la entrega de los informes de auditoria.	Puede afectar la toma de decisiones de la auditado	Deficiencia en la ejecucion y/o proceso de la auditoria	Toma de correctivos para entregar los informe sugun el cornograma	2	2	2	8	No aplicable				0
	El personal auditado no se presenta a tiempo en la auditoria.	Se presentaria retrasos en el cronograma de auditoria	Que el personal no cumple el horario y esta torpeciendo el proceso de auditoria	El auditor tenga un mejor manejo en el tiempo	2	2	2	8	No aplicable				0
	No existe una clara determinación de los objetivos de la auditoria.	No se piuede realizar un plan de auditoria adecuado	No se a determinado el alcance del plan de auditoria	Determinar el alcance para establecer el plan de auditoria	3	2	1	6	No aplicable				0

3. PLAN DE AUDITORÍA

AUDITORIA INTERNA DEL SSGCN / SGSS PLAN DE AUDITORÍA.					
Objetivo y Alcance: Verificar el cumplimiento de la norma ISO 22301:2019 / ISO 27001:2022, Verificar la eficacia y detectar oportunidad de mejora.					
Criterios de Auditoría		ISO 22301:2019 / ISO 27001:2022 y documentos de la organización			
Equipo Auditor					
Fecha	Hora	Auditor	Área/Función/Proceso/Actividad	Auditado	Lugar
27/06/2024	8 am a 9 am	EQUIPO DE AUDITORIA	Dirección Estratégica	Gerente General	Oficina Gerencia Bogotá
27/06/2024	9 am a 12 pm y 1 pm a 5 pm	NANCY SABOGAL	Monitoreo de Telecomunicaciones	Gerente de Telecomunicaciones	Sala de Junta Bogotá A1(hibrido para todas las sedes)
27/06/2024	9 am a 12 pm y 1 pm a 5 pm	DIANA CAROLINA MURCIA	Servicio de mesa de ayuda y soporte remoto a usuarios	Gerente de Mesa de Ayuda	Sala de Junta A2 (hibrido para todas las sedes)
27/06/2024	9 am a 12 pm y 1 pm a 5 pm	GABRIEL BENAVIDES	Base de datos	Gerente de Base de Datos	Sala de Junta Bogotá A3 (hibrido para todas las sedes)
28/06/2024	9 am a 11 pm	ANDRES ALFONSO	Dirección Comercial	Gerencia Comercial	Sala de Junta Bogotá A1(hibrido para todas las sedes)
28/06/2024	9 am a 11 pm	NANCY SABOGAL	Dirección de Innovación y Desarrollo	Gerencia de Innovación y Desarrollo	Sala de Junta A2 (hibrido para todas las sedes)

4. LISTA DE VERIFICACIÓN

4.CONTEXTO DE LA ORGANIZACIÓN	NO APLICA	COMPLETO	PARCIAL	NINGUNO	QUÉ TIENE?	QUE NOS FALTA	DOCUMENTOS ASOCIADOS	PROCESOS ASOCIADOS
4.1 CONOCIMIENTO DE LA ORGANIZACIÓN Y DE SU CONTEXTO			50%					
La organización debe determinar las problemáticas externas e internas que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información. NOTA: La determinación de estas cuestiones hace referencia a establecer el contexto externo e interno de la organización, considerado en el numeral 5.4,1 de la NTC-ISO 31000:2018			X		Se cuenta con un contexto, el cual se encuentra definido en: * Plan estratégico 2022-2026. * Manual de Sistema de Gestión de Seguridad de la Información , menciona el contexto de manera general. * Plan Estratégico de Tecnologías de la Información PETI 2024, en este no se referencia la Norma ISO 27001,	Se debe integrar dentro del texto lo referente a la seguridad de la información que maneja y provee a los usuarios, sobre los temas misionales. De igual manera, no se habla de las cuestiones (problemáticas externas e internas) que pueden afectar el propósito. En lo que respecta a Visión y Misión, se debe actualizar dado que en la página web, como la Intranet se presenta información diferente, versus la información contenida en Plan estratégico 2022-2026 de la entidad.	Se cuenta con el Plan Estratégico 2022-2026 Centro Nacional de Memoria histórica, el cual tiene fecha del enero 23 de 2023 con contenido de 13 páginas. https://centrodememoriahistorica.gov.co/wp-content/uploads/2023/05/PLAN ESTRATEGICO 2022-2026.pdf En el Manual del Sistema de Gestión de Seguridad de la Información SIP MA 002 Vr, 2 de 2021 ubicado en la Intranet https://intranet.centrodememoriahistorica.gov.co/visorpdf.php?id=2363&pdf=1; se indica en la página 14 se indica se encuentra documentado como parte del SGSI Pero no encontró en donde está desarrollado lo correspondiente a lo que aplica a la Seguridad de la Información. ** Plan Estratégico de Tecnologías de la Información PETI 2024, en este no se referencia la Norma ISO 27001,	
		0	1	0				
4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS			0%					
La organización debe determinar:								
a. Las partes interesadas que son relevantes al sistema de gestión de la seguridad de la información; y b. Los requisitos relevantes de estas partes interesadas				X X	En las siguientes fuentes de información: * "Estrategia de Cultura y Apropiación de TI 2023, se menciona las partes interesadas internas, pero no hay una amplia definición. *En página web/Transparencia/ 8, Información Específica para Grupos de Interés en este link se encuentra la Información para niños, niñas y adolescentes; Información para mujeres, Información para grupos étnicos. * Manual del Sistema Integrado de Gestión - Código SIP-MA-001 versión 9 (ahora versión 10 de fecha 26/04/2024) , numeral 3, Partes Interesadas en el accionara del CNMH se describe que son Victimas y organizaciones de victimas, Organizaciones sociales y de derechos humanos, Academia y centros de pensamiento, Otras entidades del Estado (Orden Nacional y Territorial), Personas desmovilizadas, Sociedad en su conjunto.	Se debe construir un documento donde se consoliden las partes interesadas, tomando las de la entidad y aquellas que puedan afectar el sistema de gestión de seguridad; así como se debe incluir los requisitos legales y reglamentarios, así como en los contractuales.	En documento "Estrategia de Cultura y Apropiación de TI 2023,publicado en la web https://centrodememoriahistorica.gov.co/wp-content/uploads/2023/04/Estrategia-de-cultura-y-apropiacion.pdf, se menciona las partes interesadas internas. De igual manera, se revisa en la página web/Transparencia/ 8, Información Específica para Grupos de Interés, en este link se encuentra la Información para niños, niñas y adolescentes; Información para mujeres, Información para grupos étnicos. Otro documento: Manual del Sistema Integrado de Gestión V9, numeral 3, Partes Interesadas en el accionara del CNMH se describe que son: Victimas y organizaciones de victimas, Organizaciones sociales y de derechos humanos, Academia y centros de pensamiento, Otras entidades del Estado (Orden Nacional y Territorial), Personas desmovilizadas, Sociedad en su conjunto. https://intranet.centrodememoriahistorica.gov.co/visorpdf.php?id=577&pdf=1	Administración del Sistema Integrado de Gestión. Gestión de Tecnología de la Información y las Comunicaciones
c. Cuales de estos requisitos pueden ser abordados a través del sistema de gestión de seguridad de la información NOTA Los requisitos de las partes interesadas pueden incluir los requisitos legales y reglamentarios, y las obligaciones contractuales.				X				

4. LISTA DE VERIFICACIÓN

5 LIDERAZGO	NO APLICA	COMPLETO	PARCIAL	NINGUNO	QUÉ TIENE?	QUE NOS FALTA
5.1 LIDERAZGO Y COMPROMISO La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información por:			31%			
a) asegurando que se establezcan la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la organización;			X		*Manual del Sistema de Gestión de Seguridad de la Información SIP-MA-002 de fecha 2021 ubicado en la intranet- En el numeral 9.1.2. Liderazgo, se menciona de forma general. * Manual del Sistema Integrado de Gestión - Código SIP-MA-001 versión 10 de fecha 26/04/2024, cuenta con un numeral 7.4. Compromiso de la Alta Dirección	Se describen varias políticas de seguridad de la información; sin embargo se debe hacer una introducción que enmarque la misionalidad, y a quienes impacta (partes internas y externas)
b) asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización;				X	Manual del Sistema de Gestión de Seguridad de la Información SIP-MA-002 de fecha 2021 , en el numeral 4, se describe el alcance, en la política no se enmarca lo descrito.	No se menciona que abarca a todos los procesos
c) asegurando que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles;				X	Se cuenta con el documento En el Manual del Sistema de Gestión de Seguridad de la Información SIP-MA-002 de fecha 2021 ubicado en la intranet	No se habla de los recursos con los que se cuenta
d) comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del sistema de gestión de la seguridad de la información;			X		Se cuenta con el documento En el Manual del Sistema de Gestión de Seguridad de la Información SIP-MA-002 de fecha 2021 ubicado en la intranet	Se debe ser mas claros y mas explicitos frente a las pretensiones de la política
e) asegurando que el sistema de gestión de la seguridad de la información logre los resultados previstos;			X		Se cuenta con el documento En el Manual del Sistema de Gestión de Seguridad de la Información SIP-MA-002 de fecha 2021 ubicado en la intranet	No se indica como se mide los resultados y cada cuanto se evalúa
f) dirigiendo y apoyando a las personas, para contribuir a la eficacia del sistema de gestión de la seguridad de la información; g) promoviendo la mejora continua, y			X X		Se cuenta con el documento En el Manual del Sistema de Gestión de Seguridad de la Información SIP-MA-002 de fecha 2021 ubicado en la intranet Se cuenta con el documento En el Manual del Sistema de Gestión de Seguridad de la Información SIP-MA-002 de fecha 2021 ubicado en la intranet	Falta realizar socializaciones e interiorización del tema de Seguridad de la Información en todos los niveles de la entidad Desde la Alta dirección, se deben generar acciones para que se mejore todo lo relacionado con el Sistema de Seguridad de la Información
h) apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidad. NOTA: La referencia a "negocio" en este documento puede ser interpretado como las actividades que son el Core o propósito de la existencia de la organización			X		Se cuenta con el documento En el Manual del Sistema de Gestión de Seguridad de la Información SIP-MA-002 de fecha 2021 ubicado en la intranet	Se debe mejorar los roles y definir los responsables, con sus obligaciones frente al cumplimiento del Sistema de Seguridad de la Información, con el fin de contribuir a la mejora continua y asegurar la información que se maneja en su misionalidad y operatividad.
	0	0	5	3		
5.2 POLÍTICA La alta dirección debe establecer una política de la seguridad de la información que:			43%			
a) sea adecuada al propósito de la organización;			X		* Manual del Sistema de Gestión de Seguridad de la Información SIP-MA-002 de fecha 2021 ubicado en la intranet. * Política de Transferencia de Información * Política de Tratamiento de la información y datos personales. * Política de Seguridad y Privacidad de la Información. *Política de Gobierno Digital. * Manual del Sistema Integrado de Gestión - Código SIP-MA-001 versión 10 de fecha 26/04/2024, cuenta con un numeral 8.5. Sistema de Gestión de Seguridad de la Información, en este se menciona que se dan lineamientos en : -Política de Transferencia de la Información. -Política de Seguridad y privacidad de la Información. -Política de Tratamiento de la Información y datos personales -Política Gobierno Digital -Manual del sistema gestión seguridad de la Información	Se deben articular todos los documentos y relacionarlos desde el manual del Sistema de Gestión de Seguridad de la Información con los demás instrumentos que se quieran crear para apalancar el cumplimiento de la norma ISO 27001.

4. LISTA DE VERIFICACIÓN

N.º	Numeral de la Norma ISO 22301:2019 SGCN	¿Qué preguntas le realizarías al auditado con respecto a este numeral de la norma?	¿Qué evidencias documentarias esperas que te muestre el auditor?
1	5.1 Liderazgo y compromiso	¿Cómo se asegura que las políticas y los objetivos de continuidad del negocio están establecidos y son compatibles con la dirección estratégica de la organización?	• Planeamiento estratégico • Matriz FODA. • Despliegue de objetivos.
3	7.2 Competencia	¿Como se determina que estas personas son competentes basándose en la educación, formación o experiencias apropiadas?	• Certificados de estudio • Certificación laboral • Prueba de conocimiento • Evaluación de desempeño
4	8.3.2 Identificación de estrategias y soluciones	¿Como se reduce la probabilidad de interrupción?	• Evaluando los riesgos. • Estrategias para hacerle frente a las interrupciones • Plan de contingencia • Identificación de factores que puede generar incidentes o accidentes

5. CASOS DE AUDITORÍA

N.º	Situación de auditoría	Numeral (es) relacionados con la norma ISO 22301:2019 / ISO 27001:2022
1	La empresa Petroleros Nacionales ha incorporado en su predio de almacenamiento de combustibles para su distribución a nivel regional, una nueva playa de carguío de combustibles, ya que a veces es necesario distribuir el producto a lugares hacia los cuales no se tiene ductos. Esta nueva playa está operando hace 6 meses. El auditor solicita los planos eléctricos, de piping (tubería) y del sistema contra incendios de la nueva playa, recibiendo la siguiente respuesta: No se cuenta con los planos, pero el área de ingeniería está pensando contratar una empresa para que haga el relevamiento y actualización de planos de todas las instalaciones, incluida la nueva playa de carguío.	
2	Auditando a la Alta Dirección de la empresa en lo relacionado al contexto de la organización, el auditor detecta que las cuestiones internas y externas identificadas tienen que ver con la parte financiera de la empresa, la continuidad del negocio y algunos aspectos relacionados con la seguridad de la información. Al respecto de la pregunta de si se han determinado cuestiones internas y externas relacionadas al proceso de gestión de riesgos el Gerente General responde que las cuestiones relevantes son las que permiten el funcionamiento de la empresa, además menciona que "los del área de riesgos probablemente han hecho un análisis al respecto".	

6. DETECCIÓN DE HALLAZGOS DE AUDITORÍA

CASO

La empresa INOVATION S.A., ofrece servicios de respaldo de información y mesa de ayuda a sus respectivos clientes. Usted forma parte del equipo de auditoría del SGSSI.

Usted saluda al Sr. Boris Bernal (responsable del SGSSI), quien será la persona que lo acompañará en su auditoría.

Al preguntar ¿cómo se controlan los documentos?, Boris indica que se ha generado un procedimiento del sistema de gestión en la empresa, en donde se ha estructurado la identificación de los documentos y registros de forma aleatoria y cada responsable de proceso tiene libertad del control.

Ud. visualiza que la política del SGSSI se ha comunicado dentro de la organización.

Ud. le pregunta a un trabajador del proceso de mesa ayuda ¿Cuál es la política del SGSSI? Éste le responde no adecuadamente el contenido de la política, el auditor escribe en su lista de chequeo que el trabajador no la sabe correctamente.

Se revisa los registros de auditoría interna con respecto al procedimiento PRO-SGSSI-003 Auditoría Interna y se encuentra conformidad de la planificación y la selección de auditores donde se constata que ellos no se auditan su propio proceso. Se evidencia programación de auditorías internas a todos los procesos y a los proveedores críticos del SGSSI, pero no se evidenció que se haya realizado auditoría interna al proceso logístico de aduanas.

Finalmente usted identifica los siguientes documentos externos necesario para prestar el servicio, tales como; Decreto de los Impuestos Nacionales, Lineamento de Cumplimiento para Operadores y Consultores N.º 1266 del año 2020 y Decreto Ministerio de TICS sobre el respaldo de la información N.º 1273 de 2019.

7. INFORME DE AUDITORÍA INTERNA

Índice

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón