Centro de Especializaciones Noeder

Diploma de Especialización Internacional

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

MÓDULO V

FORMACIÓN DE AUDITORES INTERNOS EN LAS NORMAS ISO 27001 E ISO 22301

CLASE 03

Mg. Ing. Julio Pereyra Rosales

Temario

- Plan y programa de auditorías.
- Lista de verificación auditoría.
- Seguimiento al programa de auditoría.

1. Plan y programa de auditorías

PHVA del proceso de auditoría

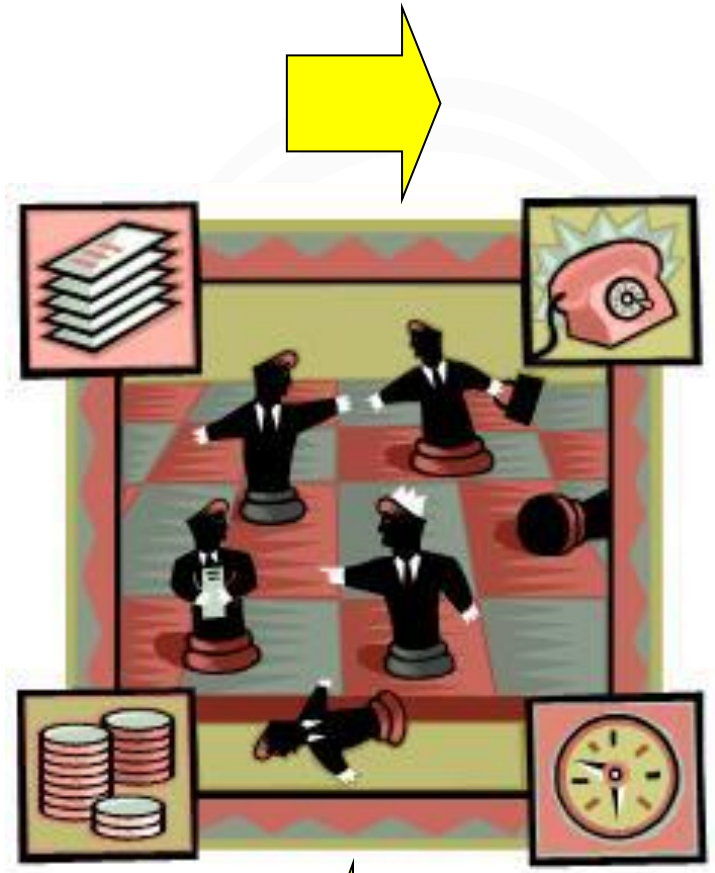
PLANEAR

Preparación de la auditoria:

Programa
Funciones
Competencias
Riesgos
Procedimiento
Recursos

HACER

Revisión Doc Plan
Doc. Trabajo
Eq. Auditor
Audit Campo
(Incl. Informe)



VERIFICAR

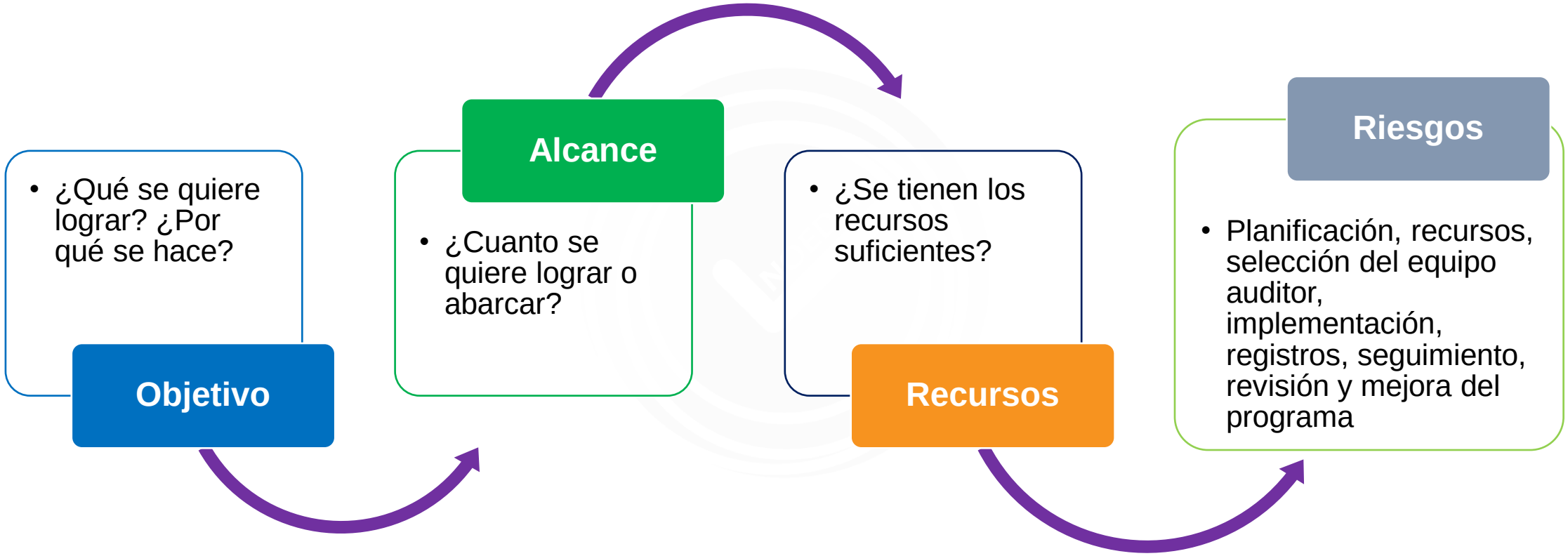
Seguimiento y revisión de resultados del Programa de auditoria

ACTUAR

Acciones de mejora del Programa

RESULTADOS

Programa de auditoría



Condiciones para auditar

Considerar:

1. Importancia de los procesos involucrados.
2. Cambios que afecten a la organización.
3. Resultados de las auditorias previas.
4. Solicitud de partes interesadas.
5. Alta incidencia de no conformidades.

Actividades de la auditoría

1. Inicio de la auditoría
2. Preparación de las actividades
3. Realización de las actividades de la auditoría
4. Preparación y distribución del informe de auditoría
5. Finalización de la auditoría
6. Actividades de seguimiento

Actividades de la auditoría

Inicio de la auditoría

Responsabilidad del equipo auditor

Establecer los contactos iniciales con el auditado

Determinar la viabilidad de la auditoría

Actividades de la auditoría

Revisar los documentos relevantes para la preparación

Preparar el plan de auditoría

Asignar el trabajo al grupo auditor

Preparar los documentos de trabajo

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)

2. Lista de verificación auditoría

Lista de Verificación

- Lista de puntos a verificar durante la auditoría.
- Recordatorio para el auditor sobre información y hechos a ser verificados.
- Sirve como guía, no debe restringir al auditor.
- Se puede preparar a manera de preguntas o usando palabras clave.
- Permitir espacio para preguntas, respuestas y valoración.
- Convertirse en un registro de auditoría.
- Herramienta útil para la administración del tiempo.

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				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
b. Los requisitos relevantes de estas partes interesadas				X				
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				

Lista de Verificación

5 LIDERAZGO	NO APLICA	COMPLETO	PARCIAL	NINGUNO	QUÉ TIENE?	QUE NOS FALTA
5.1 LIDERAZGO Y COMPROMISO		**31%**				
La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información por:						
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 explícitos 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;			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	Falta realizar socializaciones e interiorización del tema de Seguridad de la Información en todos los nivelas de la entidad
g) promoviendo la mejora continua, y				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	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		**43%**				
La alta dirección debe establecer una política de la seguridad de la información que:						
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.

Lista de Verificación

5 LIDERAZGO	NO APLICA	COMPLETO	PARCIAL	NINGUNO	QUÉ TIENE?	QUE NOS FALTA
5.1 LIDERAZGO Y COMPROMISO		**31%**				
La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información por:						
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 explícitos 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;			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	Falta realizar socializaciones e interiorización del tema de Seguridad de la Información en todos los nivelas de la entidad
g) promoviendo la mejora continua, y				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	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		**43%**				
La alta dirección debe establecer una política de la seguridad de la información que:						
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.

Lista de Verificación

5 LIDERAZGO	NO APLICA	COMPLETO	PARCIAL	NINGUNO	QUÉ TIENE?	QUE NOS FALTA
5.1 LIDERAZGO Y COMPROMISO		**31%**				
La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de la seguridad de la información por:						
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 explícitos 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;			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	Falta realizar socializaciones e interiorización del tema de Seguridad de la Información en todos los nivelas de la entidad
g) promoviendo la mejora continua, y				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	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		**43%**				
La alta dirección debe establecer una política de la seguridad de la información que:						
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.

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

3. Seguimiento al programa de auditoría

Seguimiento al programa de auditoría

¡Gracias!

Centro de
Especializaciones
Noeder

Conócenos más haciendo clic en cada botón