NTC ISO 27001-2022

metodología DE CONSULTORIA EN EL DISEÑO, PLANIFICACIÓN, DOCUMENTACIÓN, IMPLEMENTACIÓN, EVALUACIÓN Y MEJORA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE ACUERDO A LA NORMA NTC ISO/IEC 27001:2022 EN LA EMPRESA

HSEQ
Consultoría Empresarial

Estimado Sr.
Empresario en Colombia

Reciba un cordial saludo.

El desarrollo de la metodología contempla los servicios específicos, actividades y tareas a desarrollar, con el fin de establecer un ambiente de control a nivel tecnológico llevar a su organización al cumplimiento de buenas prácticas de seguridad y ciberseguridad con el fin de alcanzar un nivel idóneo de aseguramiento a los activos de TI.
Será un placer poderlos acompañar en tan importante labor, y estamos seguros de que un servicio de altos estándares de calidad genera confianza en su organización, sus colaboradores, sus clientes y demás partes interesadas el fortalecimiento del ambiente de control tecnológico de la compañía.

HSEQ
Consultoría Empresarial

OBJETIVO

Implementar el sistema de gestión de seguridad de la información de acuerdo a la norma NTC ISO/IEC 27001:2022 en la empresa a través de sesiones de acompañamiento y consultoría.

PERFIL DEL EQUIPO CONSULTOR

HSEQ
Consultoría Empresarial

Consultor Germán Sánchez

- Administrador de empresas con experiencia y competencias en habilidades gerenciales de liderazgo, dirección, planeación y desarrollo de estrategias organizacionales. Énfasis en la organización de personal y procesos, planeación estratégica, el desarrollo de estrategias de aprovisionamiento y alianzas estratégicas, gestión del riesgo, elaboración y control de presupuestos de egresos e inversiones y desarrollo de proveedores y comunicación interna y externa que fomenten el buen relacionamiento y trabajo en equipo. Alto nivel de capacidades de negociación, además de conocimientos técnicos en temas de compras, calidad, análisis de precios, políticas de compras, análisis de proveedores, indicadores de gestión, manejo de contratos, entre otros. Amplia experiencia en el diseño, ejecución, control y mejoramiento de actividades de capacitación en diferentes sistemas de gestión (ISO 9001, ISO 27001, ISO 28000, ISO 31000, entre otros) y temas de administración organizacional. Experiencia como docente de catedra universitaria en programas de pregrado, especialización y maestría en sistemas de gestión a nivel nacional. Auditor, asesor y consultor empresarial.
- Educación y formación:
  - Specialization in Management Skills – The George Washington University 2018.
  - Especialista en Sistemas de Gestión de la Calidad – Universidad Agraria de Colombia 2006.
  - Magister en Administración – Universidad Nacional de Colombia 2005
  - Administrador de Empresas – Universidad Nacional de Colombia 2001.
- Experiencia laboral:
  - Consultor senior en Sistema de Gestión .
  - ICONTEC 2008-2018. – Jefe de Abastecimiento.
  - ICONTEC 2003-2008. – Coordinador posventa y mejoramiento.
  - 15 años de experiencia en actividades de docencia universitaria en postgrados universitarios (especializaciones y maestrías) en temas relacionados a sistemas de gestión: Universidad Nacional de Colombia (Bogotá y Arauca), Uninorte (Barranquilla), Universidad de América (Bogotá), Universidad Libre (Bogotá), Universidad Santo Tomás (Bogotá, Tunja y Villavicencio), Universidad Industrial de Santander (Bucaramanga), Uniagraria (Bogotá y Yopal), ICESI (Cali), Universidad Tecnológica de Bolívar (Cartagena), Universidad Francisco de Paula Santander (Cúcuta), Universidad de Medellín (Medellín), Universidad del Cauca (Popayán), Universidad de los Llanos (Villavicencio), Universidad de Nariño (Pasto).

HSEQ
Consultoría Empresarial

Consultor Oscar Rodríguez

- Ingeniero de Sistemas, Especialista en E-Goverment, conocimiento en Gerencia y Gestión de Proyectos, Auditorías TI, Consultoría Ciberriesgos, Seguridad Informática y de la información, Aplicación controles SOX, Sistemas de Gestión de Seguridad de la Información y de Protección de datos personales (Ley 1581 de 2012), PCI DSS, Circulares Cumplimiento, Planeación estratégica TI y control interno.
- Educación y formación:
  - Ingeniero de sistemas – Universidad nacional de Colombia 2022
  - Especialista Gobierno Electrónico – Universidad Nacional de Colombia 2016
  - Auditor Líder / Implementador Líder ISO27001 – PECB 2016
- Experiencia laboral:
  - Consultor senior Risk Advisory – Deloitte (6 años)
  - Subgerente de Seguridad de la información en Multinacional (4 años)
  - Auditor Tecnología

HSEQ
Consultoría Empresarial

FACTORES CLAVES DE ÉXITO

Con el propósito de facilitar el éxito de este proyecto de implementación del sistema de gestión de la seguridad de la información en**,** se debe asegurar:

Durante la ejecución del proyecto:

1. Participación activa del líder del proceso.
2. Participación activa del equipo de apoyo del proceso.

Posterior al proyecto:

1. Adopción de los lineamientos establecidos en el proyecto.
2. Revisión periódica de resultados y toma de acciones correctivas y de mejora.

COMPROMISOS DE LAS PARTES

POR PARTE DE LA EMPRESA CONSULTORA

- Asignar a un equipo de profesionales como responsables del proyecto. Estas personas serán las interlocutoras por parte de **HSEQ Consultoría Empresarial**
- Asegurar el cumplimiento del objetivo y las actividades señaladas en este documento.
- Asistir a las reuniones de orientación y validación de resultados según la agenda acordada.
- Asegurar profesionales con las más altas competencias personales y profesionales como acompañantes en las actividades descritas.
- Garantizar absoluta confidencialidad en relación a la información obtenida durante el proceso de acompañamiento.
- Acompañar a la empresa**.** hasta el proceso de certificación por parte del ente seleccionado por la entidad.

POR PARTE DE LA EMPRESA

- Asegurar la participación activa del personal requerido para cada una de las etapas del proyecto.
- Asignar a un profesional como responsable del proyecto. Esta persona será la interlocutora por parte de la empresa
- Asistir a las reuniones de orientación y validación de resultados según la agenda acordada.
- Realizar las asignaciones que queden establecidas en cada una de las jornadas de trabajo.
- Suministrar la información necesaria para el desarrollo de las actividades planteadas.
- Garantizar que se cuentan con todos los aspectos logísticos para el desarrollo de las actividades descritas en esta metodología.

DESARROLLO DE LA metodología

ID	ETAPA	ACTIVIDADES	RESULTADOS
1	**Análisis situacional actual**	Se realizará una evaluación detallada que permita establecer el estado actual de **XXX.,** frente al cumplimiento de los requisitos normativos establecidos en la norma técnica internacional ISO 27001:2022. Para esto se usarán fuentes primarias y secundarias de información.	Diagnóstico (cualitativo y cuantitativo)
2	**Diseño del plan detallado de trabajo**	A partir de los resultados obtenidos en la etapa anterior, se diseñará un Plan Detallado de Trabajo que describa: • Las actividades a desarrollar. • Las estrategias a seguir en cada actividad. • Las responsabilidades de cada uno de los actores implicados en el SGSI. • Las fechas de iniciación y terminación de cada una de las actividades. • Los recursos necesarios para la ejecución de las actividades. • Los resultados específicos se deben obtener al final de cada una de las actividades. Nota: El Comité Directivo del Proyecto, conformado por los gerentes del proyecto de **HSEQ Consultoría Empresarial** y **Cliente**, evaluaran el esfuerzo requerido para la implementación del sistema en el alcance inicialmente previsto, frente a los recursos humanos disponibles, tanto del equipo del proyecto como de los funcionarios de la empresa y eventualmente podrían ajustar dicho alcance para lograr el objetivo de certificar el SGSI frente a ISO/IEC 27001:2022 en el plazo previsto.	Plan de trabajo detallado

DESARROLLO DE LA metodología

ID	ETAPA	ACTIVIDADES	RESULTADOS
3	**Planificación del Sistema de Gestión de Seguridad de la Información.**	Diseñar / ajustar cada uno de los elementos que constituyen la planificación del Sistema de Gestión de Seguridad de la Información en la empresa en coherencia con los propósitos fundamentales establecidos por la organización y los requisitos de la ISO 27001:2022. Revisión de la arquitectura de la seguridad existente desde las perspectivas tecnológica, física y documental y alineación con la gestión de riesgos.	Documentación relacionada a los numerales 4, 5 y 6 y del anexo A de la norma ISO 27001:2022
4	**Documentación de los procesos del Sistema de Gestión de Seguridad de la Información.**	Se realizarán / ajustarán cada uno de los documentos requeridos por el SGSI (caracterizaciones de procesos, procedimientos, registros, instructivos, guías, manuales y demás documentos de apoyo), con el fin de asegurar la conformidad de los mismos frente al referencial normativo ISO 27001:2022, los requisitos legales aplicables y los requisitos y necesidades establecidas por la empresa**.**	Documentación de los procesos del SGSI relacionada a los numerales 7 y 8 y del anexo A de la norma ISO 27001:2022.

HSEQ Consultoría Empresarial

DESARROLLO DE LA metodología

ID	ETAPA	ACTIVIDADES	RESULTADOS
5	**Implementación del SGSI**	Esta etapa de implementación aborda tres (3) ejes específicos de trabajo: 1. Divulgación de la estructura documental establecida en la etapa cuatro (4) a todos los colaboradores de los procesos que hacen parte del SGSI de la empresa**.** 2. Sensibilización y formación al personal que hace parte de los procesos del SGSI de la empresa**.** Esta formación y sensibilización estará enfocada en aspectos prácticos del SGSI que les permita adoptar e implementar la documentación en el trabajo del día a día y generar una actitud favorable hacia el mismo. **(Ver detalles en "LÍNEAS TEMÁTICAS DE FORMACIÓN EN EL SGSI").** 3. Acompañamiento en la implementación del SGSI en cada uno de los procesos de la empresa**,** que asegure la utilización apropiada de los documentos y el diligenciamiento de los registros.	Puesta en funcionamiento del SGSI en cada uno de los procesos

DESARROLLO DE LA metodología

ID	ETAPA	ACTIVIDADES	RESULTADOS
6	**Evaluación del SGSI**	Durante y posterior a la implementación del SGSI en la empresa**,** se evaluará su eficacia por medio del establecimiento e implementación de las siguientes herramientas específicas: 1. Indicadores de gestión para los objetivos del SGSI y para los procesos. 2. Revisión por la dirección. 3. Auditoría interna a TODOS los procesos del SGSI de la empresa**.**	Indicadores de gestión, revisión por la dirección, auditoría interna del SGSI
7	**Mejora del SGSI**	A partir de los resultados obtenidos en las etapas 3, 4, 5 y 6 se establecerán las acciones correctivas y de mejora necesarias para asegurar la conformidad de los procesos del SGSI en la empresa frente a los requisitos establecidos en la Norma Técnica Internacional ISO 27001:2022.	Acciones de mejora

HSEQ
Consultoría Empresarial

DESARROLLO DE LA metodología

ID	ETAPA	ACTIVIDADES	RESULTADOS
8	**Acompañamiento en el proceso de auditoría de tercera parte del organismo certificador**	Se realizará el acompañamiento en la auditoria de tercera parte desarrollada por el ente certificador y se establecerán las acciones correctivas derivadas de los resultados del proceso evaluativo.	Acciones correctivas que se puedan generar en el proceso de certificación

Tiempo para el logro del objetivo:

- El objetivo planteado se logrará en un tiempo máximo de 12 meses (teniendo en cuenta que se debe asesorar la implementación del SGSI en su totalidad), una vez se cumplan los requisitos de perfeccionamiento y legalización del contrato.
- En caso que en el diagnóstico inicial se pueda determinar un menor tiempo previsto para el proceso de implementación del SGSI, se reducirá el tiempo de asesoría según corresponda, y a su vez el valor de la inversión proporcional a los meses requeridos.

ALCANCE

Procesos objeto del alcance de certificación: Los incluidos en el mapa de procesos.

Sedes objeto del alcance de certificación: La certificación es corporativa, con un alcance en todos los procesos de la organización, y cuya sede principal está ubicada en Bogotá D.C., sede donde se realizarán y recibirán auditorías:

- Se realizará el ejercicio de auditoría interna al SGSI NTC ISO/IEC 27001:2022
- Se recibirá auditoría externa (auditoría de tercera parte del organismo certificador) al SGSI NTC ISO/IEC 27001:2022

LÍNEAS TEMÁTICAS DE FORMACIÓN EN EL SGSI

Como actividad fundamental en el proceso de acompañamiento a la implementación del SGSI en la empresa y como estrategia para garantizar su sostenibilidad a lo largo del tiempo se propone la siguiente estructura formativa al personal involucrado en los procesos:

1. **Seminario- taller:** Generalidades de un SGSI (4 horas). Líderes de procesos del SGSI.
2. **Taller:** Planificación de un SGSI (2 horas). Alta dirección, líderes de procesos del negocio.
3. **Seminario-taller:** Análisis y valoración del riesgo de seguridad de la información (4 horas). Líderes de procesos negocio y SGSI. Gestión de riesgos.
4. **Sensibilización SGSI:** (1 hora). Múltiples sesiones, todo el personal.
5. **Seminario-taller:** Herramientas de evaluación y mejora del SGSI (2 horas). Alta dirección, líderes de procesos, Sistemas de Gestión
6. **Seminario:** Aspectos claves para abordar de manera exitosa la auditoria de certificación (2 horas)

HSEQ
Consultoría Empresarial

LÍNEAS TEMÁTICAS DE FORMACIÓN EN EL SGSI

NOTAS:

1. Cada uno de los seminarios incluyen memorias para los participantes y certificados de asistencia.

2. En relación a la certificación: se emitirá certificado de asistencia al participante que acredite asistencia del 100% al taller.

3. El número máximo de participantes en cada uno de los seminarios señalados en esta metodología no podrá superar las 30 personas. La entidad se encargará de seleccionar a dichos participantes.

4. La empresa se encargará de todos los aspectos logísticos necesarios para la ejecución de estos seminarios de formación.

5. Las fechas y los horarios de cada uno de los seminarios serán acordados entre las dos partes.

HSEQ
Consultoría Empresarial

GRACIAS

HSEQ
Consultoría Empresarial