Proyecto
Auditoría

SGI basado en SGC y SGSI

Participantes:

Iván Álvarez
Andrea Siles
Edgar Andrés

Proyecto

La norma

Introducción

La normas ISO 27001, e ISO 9001 se basan en el ciclo de Deming, como bien sabemos consiste en Planificar-Hacer-Verificar-Actuar (PHVA) y puede ser aplicado a todos los procesos. La metodología PHVA se puede describir de la siguiente forma:

- Planificar: se establecen los objetivos y los procesos necesarios para conseguir resultados según las necesidades de los clientes y la política de seguridad de la organización.
- Hacer: se implantan los procesos.
- Verificar: se revisan y se evalúan tanto lo servicios como los procesos comparándolos con las políticas, los objetivos y los requisitos de información sobre los resultados.
- Actuar: comienzan a emprender acciones para mejorar el rendimiento del Sistema de Gestión calidad y seguridad de forma continua.

Implantación de un SGI

Implantación de un SGC según ISO 9001

La norma ISO 9001 es una norma de ámbito internacional que tiene como finalidad proporcionar a las organizaciones los elementos de un Sistema de gestión de la calidad efectivo, dándoles un marco de referencia para gestionar de una manera eficaz y satisfactoria las necesidades de sus clientes y otras partes interesadas.

Sus objetivos son:

- mejorar la satisfacción de los clientes
- incrementar la tasa de fidelización de los mismos.
- Aumentar los riesgos y la cuota de mercado obtenida.
- Mayor flexibilidad y capacidad de respuesta frente a las oportunidades de mercado.
- Integración y alineación de los procesos internos, que dará lugar a un aumento de la productividad y una mejora en los resultados.
- Rendimiento empresarial mejorado.
- Mayor eficiencia en la gestión de costes.
- Incremento del nivel de confianza con respecto a las partes interesadas en cuanto a la coherencia, la eficacia y la eficiencia de la organización.
- Aumento de la credibilidad y la competitividad en el mercado.
- Mayor consistencia en la entrega del producto o servicio.
- Menores costos y tiempos de ciclo más cortos, gracias a un uso más eficaz de los recursos.
- Mejora de los procesos de comunicación, planificación y administración.

Implantación de un SGSI según ISO 27001

La norma ISO 27001 es una norma de ámbito internacional que tiene como finalidad proporcionar a las organizaciones los elementos de un Sistema de gestión de la seguridad, para gestionar la seguridad de la información de manera planificada y ordenada, anticipándonos a los problemas que puedan surgir.

Sus objetivos son:

- Ser coherentes con la política de seguridad de la información
- Ser medibles
- Tener en cuenta los requisitos de la seguridad de la información aplicada y los resultados de la valoración y el tratamiento de los riesgos
- Ser comunicados
- Ser actualizados según sea necesario

Etapas

Para implantar un SGI según las normas ISO 27001 e ISO 9001, el ciclo PDCA se basa en la realización constante de cuatro pasos, se deben seguir los pasos siguientes:

- Comprensión de la organización y su contexto.
- Comprensión de las necesidades y expectativas de las partes interesadas.
- Determinación del alcance de los sistemas de gestión de calidad y de gestión de la seguridad.
- Definición de la política de seguridad y de calidad.
- Requisitos legales y otros requisitos.
- Definición de objetivos de calidad y seguridad a conseguir y definición del programa de gestión de calidad y seguridad.

Planear

En esta etapa realizaremos análisis cuantitativos, reuniones, grupos de consenso, todo lo requerido para así definir como mínimo actividades, responsables, tiempos y planificación temporal .

- Recursos (Estructura y responsabilidades).
- Competencia y toma de conciencia.
- Comunicación.
- Información documentada del SGC y del SGSI (creación, actualización y control).
- Planificación y Control operacional.

Hacer

Realizamos cada una de las actividades planteadas ,teniendo en cuenta los parámetros establecidos (recursos ,riesgos, tiempos) según la complejidad del plan de acción se puede considerar hacer cambios a una pequeña escala o prueba piloto.

- Seguimiento, medición, análisis y evaluación.
- Evaluación del cumplimiento.
- Auditoria del SGC y SGSI.
- Revisión por la dirección.

Verificar

Aqui nos haremos la pregunta ¿En que medida se cumplio lo planificado?, debemos verificar el cumplimiento de las actividades y en general, definimos si el plan de acción se consigue el resultado esperado y se logró el efecto deseado (eficacia del plan).

- No conformidad y acción correctiva.
- Mejora continua.
- Certificación del SGSI y SGC.

Actuar

En este paso, nos fijamos en las desviaciones entre lo planificado y lo realizado se bordan en esta etapa al cerrar las brechas evidenciadas en la verificación.

- Aplicar acciones correctivas.
- Revisión interna del SGSI y SGC.

Planificación

Comprensión de la Organización y su Contexto

La organización debe determinar las cuestiones, tanto externas como internas, que son pertinentes para su propósito y que pueden afectar a su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad y calidad.

Características o condiciones internas de la organización, tales como sus actividades, productos y servicios, dirección estratégica, cultura y capacidades (personas, conocimientos, sistemas,...).

Las cuestiones internas y externas dan lugar a riesgos y oportunidades para la organización.

La organización debe identificarlos y evaluarlos, a fin de determinar las acciones necesarias para abordarlos y gestionarlos.

Comprensión de las Necesidades y Expectativas de las Partes Interesadas

La organización debe determinar:

1. Las partes interesadas que son pertinentes a los sistemas de gestión de calidad e información.

2. Las necesidades y expectativas pertinentes de dichas partes interesadas. Cuáles de estas necesidades y expectativas se convierten en requisitos.

Determinación del Alcance del SGI

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad y calidad para establecer su alcance, teniendo en cuenta las cuestiones externas e internas (contexto de la organización); requisitos legales y otros requisitos aplicables: unidades, funciones y límites físicos de la organización; actividades, productos y servicios; autoridad y capacidad para ejercer control e influencia.

Una organización tiene libertad y flexibilidad para definir dichos límites. Todas aquellas actividades, productos y servicios que estén dentro de este alcance, deberán incluirse en el sistema de gestión calidad y seguridad. El alcance del sistema debe mantenerse como información documentada y estará disponible para las partes interesadas.

Política Integrada

El siguiente paso consiste en la elaboración de una política calidad y seguridad por parte de la dirección de la empresa. La política de calidad y seguridad es un documento público preparado por la dirección de la empresa en el cual se describen sus compromisos respecto a su actuación para garantizar la calidad y la seguridad

En este documento se basarán sus objetivos y metas de calidad y seguridad. La definición de política que da la norma es la siguiente: “Declaración por parte de la organización sobre sus intenciones y principios de acción acerca de su actuación para garantizar la calidad y la seguridad, que le proporciona un marco general de actuación en el que se fundamentan sus objetivos y metas”.

Identificación de Aspectos

En la norma se dice que la organización dentro del alcance definido del sistema de gestión de calidad y seguridad, debe determinar los aspectos de calidad y seguridad de sus actividades, productos y servicios que puede controlar y de aquellos en los que puede influir.

Requisitos Legales y Otros Requisitos

Los requisitos legales y otros requisitos pueden surgir de requisitos obligatorios, tales como leyes y reglamentaciones aplicables, o de compromisos voluntarios, tales como normas de organizaciones o de la industria, relaciones contractuales, códigos de buenas prácticas.

La organización debe identificar y tener acceso a todos los requisitos legales y reglamentarios aplicables a los aspectos calidad y seguridad de sus actividades, productos y servicios.

Para asegurar el cumplimiento legal, es necesario asegurarse previamente de conocer todos los requisitos legales que son aplicables y hacerlo con una periodicidad adecuada.

La legislación aplicable puede ser de ámbito europeo, nacional, autonómico o local. La organización debe mantener información documentada sobre sus requisitos legales y otros requisitos.

Este procedimiento debe comprender también aquellos requisitos que la organización haya suscrito como obligatorios, así como los posibles acuerdos establecidos con la administración u otros órganos sociales, en el caso de que existan.

Definición de Objetivos del SGI

La organización debe establecer objetivos calidad y seguridad para las funciones y niveles pertinentes, teniendo en cuenta los aspectos calidad y seguridad significativos de la organización y sus requisitos legales y otros requisitos asociados, y considerando sus riesgos y oportunidades.

- Los objetivos de calidad y seguridad deben:
- Ser coherentes con la política de calidad y seguridad
- Ser medibles (si es posible)
- Ser objeto de seguimiento
- Comunicarse
- Actualizarse, según corresponda.

Los objetivos de calidad y seguridad se deben comunicar a las personas que trabajan bajo el control de la organización y que tengan capacidad para influir en el logro de dichos objetivos.

La organización debe conservar información documentada sobre los objetivos. Las organizaciones deben establecer indicadores de calidad y seguridad para cuantificar objetivos y metas. Estos deben ser tales que permitan medir los impactos en la calidad y seguridad, puedan ser evaluados internamente y verificados externamente, pueda seguir su evolución en el tiempo o con relación a normas establecidas.

La organización debe establecer y mantener al día un programa para lograr sus objetivos y metas.

Objetivos

•Fines de calidad y seguridad generales que la organización pretende alcanzar, basados en la política de calidad y seguridad y en los aspectos de calidad y seguridad significativos, y cuantificados siempre que sea posible.
•Estos objetivos deben establecerse claramente y sin ambigüedades, deberían concordar con la política de calidad y seguridad y conducir al compromiso de mejora continua.

Metas

•Requisitos detallados de actuación, cuantificados siempre que sea posible, aplicados a la organización o parte de esta, que tienen su origen en los objetivos de calidad y seguridad y se deben cumplir para alcanzar dichos objetivos.

Implantación

Recursos (Estructura y Responsabilidades)

La organización debe determinar y proporcionar los recursos (humanos, técnicos y financieros) necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGC y SGSI.

La empresa debe definir y documentar funciones, responsabilidades y autoridad para conseguir una gestión de calidad y seguridad eficaz. La dirección debe designar un representante que, independientemente de otras responsabilidades, tenga autoridad y responsabilidad definidas para asegurar que se cumplen y mantienen al día los requisitos de las normas e informar a la dirección sobre el funcionamiento del sistema para su revisión y mejora.

El representante de la gestión de la calidad y seguridad deberá informar a la dirección del comportamiento del sistema, incluyendo las recomendaciones para su mejora.

Competencia y Toma de conciencia

La dirección de la empresa debe transmitir a sus empleados los valores de calidad y seguridad de la información de la organización y comunicarles su compromiso a través de la política integrada.

El personal con funciones específicas debe estar cualificado por sus estudios, formación posterior o experiencia para llevar a cabo los requisitos de calidad y seguridad de la información.

El personal cuyo trabajo puede ocasionar riesgos debe haber recibido formación suficiente y tomar conciencia de:

1. La importancia de la conformidad con la política integrada y los procedimientos de calidad y seguridad de la información, y con los requisitos de SGI.

2. Los riesgos significativos, reales o potenciales de sus actividades de trabajo y los beneficios derivados de un mejor comportamiento personal.

3. Sus funciones y responsabilidades para lograr conformidad con la política y los procedimientos de calidad y seguridad de la información y con los requisitos del SGI.

4. Las posibles consecuencias en caso de apartarse de los procedimientos de operación especificados

Para cada puesto se debe recoger la cualificación necesaria en materia de calidad y seguridad de la información. La organización debe disponer de una sistemática para detectar las necesidades de formación (entre el personal existente y nuevas contrataciones) y elaborar planes de formación adecuados. Se debe hacer un seguimiento y evaluación de dicha formación, así como mantener registros de dicha formación.Este apartado es aplicable a todas las personas que desarrollen su actividad para o en la organización, lo que incluye subcontratistas o cualquier persona que desarrolle su actividad para la organización, directa o indirectamente. Se debe registrar y mantener ,la información sobre la formación, aprendizaje y experiencia de todas las personas identificadas.

Comunicación

La empresa debe establecer, implementar y mantener los procesos necesarios para la comunicación tanto interna como externa pertinente al SGI, que incluyan: qué comunicar, cuándo comunicar, a quién comunicar y cómo comunicarlo.

La comunicación interna se refiere a la que mantiene la empresa con sus trabajadores para motivarlos y animarlos a llevar a cabo una mejor actuación integrada teniendo en cuenta la calidad y la seguridad de la información.

La comunicación externa será la que se mantiene con partes interesadas como: vecinos, clientes, autoridades competentes, público en general, etc. Para mantener el compromiso público con la calidad y la seguridad de la información en cuyo caso deberá registrar dicha decisión al respecto y definir métodos para realizar dicha comunicación pública.

Información Documentada del SGI (creación, actualización y control)

La organización debe establecer y mantener actualizada la información, en papel o soporte informático, para describir los SG y las relaciones entre los diferentes elementos y proporcionar información sobre otros documentos relacionados.

En ella se incluyen:

- Manual de gestión de la calidad y seguridad donde se plasma la política de calidad y seguridad, se definen las responsabilidades y los objetivos, metas y programas. Indica lo que hace la empresa para cumplir los requisitos de la norma.

- Procedimientos e instrucciones técnicas donde se describen cómo se realizan las distintas actividades de la empresa.

- Otros procedimientos como Planes de auditorías, Planes de formación, Programas, Normativa, etc.

- Registro de incidentes, quejas, etc. Con los que se demuestra que se están cumpliendo los requisitos del sistema.

La documentación se estructura en forma de pirámide. En la base se sitúan las instrucciones técnicas que utilizan diariamente los trabajadores, y en la cúspide el manual que recoge los principios básicos del sistema. En un nivel intermedio se encontrarán los procedimientos.

El manual nos indica que se hace en la organización para alcanzar los requisitos de la norma, mientras que los procedimientos nos indican cómo lo hace y las instrucciones técnicas llevan los procedimientos hacia direcciones concretas para cada parte del proceso productivo.

Los registros, por su parte, permiten demostrar que se están cumpliendo los requisitos del sistema. Un procedimiento suele constar de los siguientes apartados:

- Objeto
- Alcance
- Definición y abreviaturas
- Desarrollo
- Responsabilidades
- Anexos (formularios, registros, etc.)

La información documentada requerida por el sistema de gestión de calidad y seguridad y por la norma se debe controlar para asegurarse de que:

- Esté disponible y sea idónea para su uso, dónde y cuándo se necesite
- Esté protegida adecuadamente

Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

- Distribución, acceso, recuperación y uso
- Almacenamiento y preservación
- Control de cambios (versiones)
- Conservación y disposición

Planificación y Control Operacional

El control operacional está formado por la documentación generada para identificar y controlar aquellas operaciones y actividades relacionadas con los aspectos de calidad y seguridad significativos identificados.

El tipo y la extensión de los controles operacionales dependen de la naturaleza de las operaciones, de los riesgos y oportunidades, de los aspectos calidad y seguridad significativos y de los requisitos legales y otros requisitos. Cada organización tiene flexibilidad para seleccionar el tipo de métodos de control operacional necesarios para asegurar que los procesos sean eficaces para el logro de los objetivos deseados.

Estos métodos pueden incluir:

- diseñar unos procesos de manera que se prevengan errores y se aseguren resultados coherentes, usar tecnologías para controlar los procesos y prevenir resultados adversos, usar personal competente, llevar a cabo los procesos de una manera especificada,realizar un seguimiento o medición de los procesos para verificar los resultados

- La organización decide el grado de control necesario dentro de sus propios procesos (por ejemplo el proceso de compras) para controlar o influir en los procesos controlados externamente o en los proveedores de productos o servicios. Planificará estas actividades para asegurarse que cumple con los requisitos establecidos:

Preparación y Respuesta ante Emergencias

Los accidentes que pueden producirse en una empresa (riesgos) pueden tener graves consecuencias para la seguridad de los trabajadores, así como generar pérdidas económicas para la organización o incluso la pérdida de la sostenibilidad empresarial.

La organización debe estar preparada para responder a situaciones de emergencia de una manera apropiada. Es necesario prevenir estas situaciones y para ello se deben poner en funcionamiento planes para que la empresa lleve a cabo una actuación correcta ante las emergencias, por tanto debe gestionarse el riesgo identificando primeramente y posteriormente estableciendo directrices de prevención, contingencia y restauración.

Por tanto se considerará el siguiente programa de prevención de riesgos:

1. Identificación y evaluación de riesgos potenciales y situaciones de emergencia.

2. Prevención de riesgos mediante: Acciones requeridas para prevenir o mitigar los riesgos.

3. Aprendizaje basado en experiencias de riesgos anteriores.

4. La empresa debe crear procedimientos, responder a posibles riesgos y situaciones de emergencia, y evitar las consecuencias asociadas.

5. El plan de restauración debe permitir mitigar cualquier efecto asociado de las emergencias identificadas..

6. Establecer simulacros para asegurar que los planes funcionan, y revisar los procedimientos periódicamente.

Evaluación Del Desempeño

Seguimiento, Medición, Análisis y Evaluación

La organización debe hacer seguimiento, medir, analizar y evaluar su desempeño en cuanto a calidad y seguridad de la información. Para ello debe determinar: qué necesita seguimiento y medición, los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para que los resultados sean válidos, criterios para evaluar su desempeño de calidad y seguridad de la información y los indicadores apropiados, cuándo realizar el seguimiento y la medición, cuándo se deben analizar y evaluar los resultados del seguimiento y medición.

Cuando se determina a qué se debe hacer seguimiento y qué se debería medir, además del progreso de los objetivos ambientales, se debe tener en cuenta los aspectos ambientales significativos, los requisitos legales y otros requisitos y los controles operacionales.

Es importante asegurar que los equipos utilizados para el seguimiento y medición están calibrados o verificados correctamente.

La organización debe evaluar su desempeño y la eficacia de su SGI. Se debe conservar información documentada apropiada como evidencia de los resultados de medición, análisis y evaluación.

Se establecerán los procedimientos para llevar a cabo un seguimiento y medir las características claves. Debe existir un sistema para medir y verificar la actuación de calidad y seguridad de la información, confrontando con los objetivos y metas en las áreas correspondientes.

Las actividades de seguimiento y medición se concretan en:

- Control y medición de las características claves de las operaciones y actividades con riesgo significativo

- Calibración y mantenimiento de los equipos de inspección

- Evaluación del cumplimiento de la legislación y reglamentación ambiental aplicable

- Establecimiento y actualización de los procedimientos y registros pertinentes.

Evaluación Del Cumplimiento

La empresa debe establecer, implementar y mantener al día los procesos necesarios para la evaluación periódica de cumplimiento de la legislación y reglamentación de calidad y seguridad aplicable y otros requerimientos a los que se someta, manteniendo información documentada como evidencia de los resultados de la evaluación del cumplimiento.

Auditoria Interna Del SGI

Una auditoría es un proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

La empresa debe llevar a cabo auditorías internas a intervalos planificados para obtener información acerca de la conformidad del sistema (con los requisitos propios de la organización para su SGC y SGSI y con la normas ISO 9001 e ISO 27001) y de la implementación y mantenimiento eficaz del mismo.

Para ello establecerá uno o varios programas de auditoría interna que recogerán: frecuencia de realización de las auditorías, métodos, responsabilidades, requisitos de planificación y de elaboración de los informes correspondientes a dichas auditorías internas.

El objetivo de estas auditorías es determinar si el sistema de gestión de calidad y seguridad cumple con los planes establecidos y suministrar información sobre los resultados de las auditorías a la Dirección. Se pueden realizar por auditores internos o externos y se debe asegurar la independencia del auditor.

Se debe conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de la misma. Las no conformidades detectadas durante las auditorías deben ser objeto de acciones correctivas apropiadas.

En la norma ISO 19011 se establecen los requisitos para el establecimiento de un programa de auditoría interna, sobre cómo deben realizarse las auditorías internas y sobre la evaluación de la competencia de las personas que realizan la auditoría.

Revisión Por La Dirección

Una vez que se ha implantado el sistema y se ha comprobado, la alta dirección de la organización debe revisar el SGI con una frecuencia determinada, para comprobar que sigue siendo apropiado y eficaz, y que cumple con el compromiso de mejora continua.

En la revisión se deben establecer unos elementos de entrada para que la dirección pueda evaluar el sistema de forma eficaz. En función de esta información, la dirección establecerá conclusiones sobre la conveniencia, adecuación y eficacia del SGI y tomará las decisiones oportunas (sobre las oportunidades de mejora continua, necesidades de cambios en el SGI, acciones necesarias si no se han logrado los objetivos, cualquier implicación para la dirección estratégica de la organización).

La organización debe conservar información documentada como evidencia de los resultados de la revisión del SGI por la dirección.

Mejora

No Conformidad Y Acción Correctiva

El sistema de gestión de calidad y seguridad no funciona perfectamente, en ocasiones se producen fallos por diferentes motivos: fallos en las instalaciones, errores humanos, fallos del propio sistema de gestión, etc. Una no conformidad es un incumplimiento de un requisito.

Cuando ocurra una no conformidad se debe:

- reaccionar ante la no conformidad y cuando sea aplicable o tomar acciones para controlarla y corregirla o hacer frente a las consecuencias, evaluar la necesidad de acciones para eliminar las causas de la no conformidad (para que no vuelva a ocurrir), mediante: la revisión de la no conformidad o la determinación de las causas de la misma o el análisis de si existen no conformidades similares (o potenciales) implementar cualquier acción necesaria revisar la eficacia de las acciones correctivas tomadas, si fuera necesario, hacer cambios en el SGI.

- Las acciones correctivas deben ser apropiadas a la importancia de los efectos de las no conformidades encontradas. Se debe mantener información documentada de las no conformidades detectadas, de las acciones tomadas posteriormente y de los resultados de las acciones correctivas.

Mejora Continua

La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del SGI para mejorar su desempeño global. Para ello será necesario mejorar continuamente los subsistemas SGC y SGSI que lo componen.

Es la propia organización la que determina el ritmo, el alcance y los tiempos de las acciones que apoyan la mejora continua contando con indicadores del sistema para determinar los puntos del mismo en los que el desempeño es bajo.

El desempeño de calidad y de seguridad de la información se puede mejorar aplicando el SGI como un todo o mejorando uno o más de sus elementos en función de los indicadores.

Este proceso es estratégico para garantizar la sostenibilidad empresarial de cualquier empresa moderna y poder así sobreponerse al mercado global y competitivo del siglo XXI.

Conclusión

Certificación del SGI

La certificación es la acción llevada a cabo por una entidad reconocida como independiente de las partes interesadas manifestando que se dé la confianza adecuada de que un producto, proceso o servicio, debidamente identificado es conforme con una norma específica u otro documento normativo.

El proceso de certificación del sistema de gestión de calidad y seguridad según ISO 27001 y la ISO 9001 se indica a continuación.

Los pasos a seguir para que una empresa pueda certificar su SGI son:

- Implantar un SGC conforme a la norma ISO 9001
- Implantar un SGSI conforme a la norma ISO 27001
- Remitir a un organismo de certificación acreditado la solicitud para obtener las certificaciones pertinentes
- Vista previa del organismo de certificación que se ha elegido a la empresa y análisis de la documentación pertinente
- Proceso de auditoría realizado por el organismo de certificación
- Concesión de la certificación a la empresa
- El organismo de certificación acreditado asignará un número de registro a la empresa
- La empresa ya está en disposición de utilizar el logotipo indicativo de certificación en su SGC y SGSI

Marca de Certificación del SGI

Es el distintivo usado por las organizaciones certificadas para hacer público que poseen un SGC y un SGSI implantado según las normas ISO 9001 e ISO 9001. El poseer este símbolo significa:

- El establecimiento y funcionamiento de sus sistemas de gestión
- El compromiso de mejorar su servicio y conformidad con los clientes y la seguridad de sus datos y de establecer una evaluación sistemática, objetiva y periódica más allá de los requisitos establecidos por la legislación.
- La participación activa de los empleados.

Esta marca tiene por objetivo aumentar el conocimiento de esta referencia entre el público y las partes interesadas.. Además permite que las empresas que se certifican como ISO 9001 e ISO 27001 tengan una mejor comunicación en el mercado.

El distintivo de certificación ISO 9001 e ISO 27001 se puede usar en información anunciando la certificación de la empresa, en membretes de la organización certificada y en cualquier tipo de publicidad siempre que se mencione la empresa y no sean exclusivamente anuncios de productos y marcas comerciales de la empresa.

Las certificaciones siempre son un símbolo de excelencia que otorga reconocimiento y garantías a los clientes de un buen servicio y profesionalidad.

Glosario

1. Sistema de gestión integrado (SGI): conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas, y objetivos y procesos para el logro de estos objetivos.

2. Sistema de gestión de calidad (SGC): parte del sistema de gestión usada para gestionar aspectos de calidad, cumplir los requisitos legales y otros requisitos, abordar los riesgos y aprovechar oportunidades.

3. Sistema de gestión de seguridad de información (SGSI): parte del sistema de gestión usada para gestionar aspectos de calidad, cumplir los requisitos legales y otros requisitos, abordar los riesgos y aprovechar oportunidades.

4. Política integrada: intenciones y dirección de una organización, relacionadas con el desempeño global, como las expresa formalmente su alta dirección.

5. Política de calidad: intenciones y dirección de una organización, relacionadas con el desempeño de calidad, como las expresa formalmente su alta dirección.

6. Política de seguridad de la información: intenciones y dirección de una organización, relacionadas con el desempeño de seguridad de la información, como las expresa formalmente su alta dirección.

7. Organización: persona o grupo de personas que tienen sus propias funciones y responsabilidades, autoridades y relaciones para el logro de sus objetivos.

8. Parte interesada: persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad. (Ej. Clientes, proveedores, ONGs, empleados,...).

9. Ciclo de vida: etapas consecutivas e interrelacionadas de un sistema de producto (o servicio), desde la adquisición de materia prima o su generación a partir de recursos naturales (o personales) hasta la disposición final. Estas etapas incluyen: adquisición de materias primas, diseño, producción, transporte/entrega, uso, tratamiento al finalizar la vida y la disposición final.

10. Proceso: conjunto de actividades interrelacionadas o que interactúan, que transforman las entradas en salidas.

11. Auditoría: proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoria.

12. Mejora continua: actividad recurrente para mejorar el desempeño.

13. Desempeño de calidad: desempeño (resultado medible) relacionado con la gestión de aspectos de calidad.

14. Desempeño de seguridad de la información: desempeño (resultado medible) relacionado con la gestión de aspectos de seguridad de la información.

15. Requisitos legales y otros requisitos: requisitos (necesidad o expectativa establecida, generalmente implícita u obligatoria) legales que una organización debe cumplir y otros requisitos que una organización decide cumplir.

Plan Auditoría

A continuación se expone el plan que se utilizará para la auditoría externa acerca de la presente norma integrada sobre calidad y seguridad de la información, primeramente se definirá el alcance de la misma, posteriormente se definirán los criterios a evaluar, llegados a este punto se explicitan los documentos necesarios para la verificación de criterios y se procede a la revisión, en este caso se proveen observaciones para concretar las causas / efectos de la no consecución de criterios, y así concienciar de la necesidad de mejora, por último se adjunta una conclusión global del estado del proyecto en cuanto a criterios de calidad y seguridad de la información.

Alcance

En esta etapa explicitamos las áreas sobre las que se aplicará la evaluación de criterios para poder cuantificar la consecución de SGI compuesto de un SGC y SGSI, para lo que exigimos como previamente se ha explicitado:

General

- Comprensión de la organización y su contexto.
- Comprensión de las necesidades y expectativas de las partes interesadas.
- Determinación del alcance de los sistemas de gestión de calidad y de gestión de la seguridad.
- Definición de la política de seguridad y de calidad.
- Requisitos legales y otros requisitos.
- Definición de objetivos de calidad y seguridad a conseguir y definición del programa de gestión de calidad y seguridad.

Planear

- Recursos (Estructura y responsabilidades).
- Competencia y toma de conciencia.
- Comunicación.

- Información documentada del SGC y del SGSI
- Planificación y Control operacional.

Hacer

- Seguimiento, medición, análisis y evaluación.
- Evaluación del cumplimiento.
- Auditoria del SGC y SGSI.
- Revisión por la dirección.

Verificar

- No conformidad y acción correctiva.
- Mejora continua.
- Certificación del SGSI y SGC.

Actuar

- Aplicar acciones correctivas.
- Revisión interna del SGSI y SGC.

Tras la comprobación de los criterios obtenidos a partir de dichas premisas se espera proveer una serie de evidencias eficaces y cuantificables para determinar el grado de obtención de calidad y seguridad de la información según normas ISO 9001 y 27001.

criterios

- Comprensión de la organización y su contexto, para poder verificar este criterio se solicitará el documento de constitución de grupo y se comprobará si existe una clara designación de estructura, responsabilidad y comunicación.
  (Coordinador y equipo se han designado correctamente,se ha seguido alguna norma)

- Comprensión de las necesidades y expectativas de las partes interesadas, para poder verificar este criterio se solicitará el documento de objetivos y se comprobará si se alinean con los establecidos para la entrega del trabajo colaborativo.
  (Se han comunicado los objetivos responsabilidades y fechas,se han comunicado nombramientos)

- Determinación del alcance de los sistemas de gestión de calidad y de gestión de la seguridad, para poder verificar este criterio se solicitará el documento de alcance y se comprobará si existen tareas de revisión (en cuanto calidad), y se solicitará una justificación de medidas de seguridad tomadas durante el desarrollo, se comprobará que existen al menos dos (en cuanto a seguridad).(Se ha acordado el alcance)

- Definición de la política de seguridad y de calidad, para poder verificar este criterio se solicitará el documento de constitución de grupo y se comprobará si existen valores relacionados con la consecución del calidad y seguridad de la información.

- Requisitos legales y otros requisitos, para poder verificar este criterio se solicitará el documento de análisis legal y se comprobará si se contemplan LSSI, LOPD y RGPD,.(Se contemplan requisitos legales de seguridad sin afectar el rendimiento,existe opción de aceptar Términos)

- Definición de objetivos de calidad y seguridad a conseguir y definición del programa de gestión de calidad y seguridad, para poder verificar este criterio se solicitará el documento de objetivos y se comprobará si se establecen objetivos / metas de seguridad de la información y calidad.

- Recursos (Estructura y responsabilidades), para poder verificar este criterio se solicitará el documento de constitución de grupo y se comprobará si la estructura es adecuada para el tipo de proyecto, en este caso se considera adecuada la horizontal por características del equipo y su organigrama, asimismo se comprobará si todos los componentes tienen una responsabilidad definida.

- Competencia y toma de conciencia, para poder verificar este criterio se solicitará el registro de comunicación de grupo y se comprobará si se ha concienciado exhaustivamente a los diferentes componentes del grupo sobre sus tareas, se considerará correcto la llamada de atención dos veces por semana.

- Comunicación, para poder verificar este criterio se solicitará el registro de comunicación de grupo y se comprobará si existe dicho documento.
  (Existe constitución de grupo,existen actas de reunión,se ha planificado,se ha gestionado el proyecto)

- Información documentada del SGC y del SGSI, para poder verificar este criterio se solicitará la documentación del proyecto y se comprobará que siga una estructura con los siguientes apartados: introducción, análisis de alternativas, objetivos, alcance, gestión de riesgos, planificación temporal, evaluación económica y conclusión.(La documentación es consistente)

- Planificación y Control operacional, para poder verificar este criterio se solicitará la documentación del proyecto y se comprobará que en el apartado de alcance se realice una estimación de tiempos y se definan los tiempos reales de cada tarea (en caso de encontrarse en otro apartado se considera válido), y se comprobará que en el apartado temporal se haya realizado un diagrama Gantt de manera consistente respecto al alcance.(Existe índice y se han rellenado todos los puntos estipulados)

- Seguimiento, medición, análisis y evaluación, para poder verificar este criterio se solicitara el alcance del proyecto y se comprobará la existencia de procedimientos / tareas destinadas a seguimiento, medición, análisis y evaluación de manera integrada o individualmente.(Existe captura de requisitos,análisis de alternativas y elección,se ha diseñado UML,son cuantificables y concretos los requisitos,existen casos de uso,existen prototipos de interfaces,el diseño cumple los requisitos)

- Evaluación del cumplimiento, para poder verificar este criterio se solicitara el alcance del proyecto y se comprobará que la tarea que involucra evaluación de resultados obtenidos cuenta con una rúbrica alineada con los objetivos del proyecto.

- Auditoria del SGC y SGSI, para poder verificar este criterio se solicitara el registro de actas de reunión y se comprobará si se han realizado al menos dos en la consecución del proyecto.

- Revisión por la dirección, para poder verificar este criterio se solicitara el registro de comunicación y el documento de constitución de grupo, y se comprobará si se han establecido un coordinador y este ha comunicado a su vez al menos dos veces errores contemplados en cualquier tarea.

- No conformidad y acción correctiva, para poder verificar este criterio se solicitará el documento de gestión de riesgos y se comprobará la existencia de un plan de emergencia (o similar).

- Mejora continua, para poder verificar este criterio se solicitará el documento de gestión de riesgos y se comprobará la existencia de un plan de restauración (o similar).

- Certificación del SGSI y SGC, para poder verificar este criterio se solicitará la documentación del proyecto y se comprobará si existe una mención / compromiso explícito con la calidad y seguridad de la información (en algún punto).

- Aplicar acciones correctivas, para poder verificar este criterio se solicitará el registro de incidencias del proyecto y se comprobará si se explicita tanto el riesgo como la acción correctiva desplegada.

- Revisión interna del SGSI y SGC, , para poder verificar este criterio se solicitara el registro de comunicación y se comprobará si se comunicado al menos una vez alguna consideración de seguridad de la información o calidad.

Ejecución

revisión

En la siguiente tabla se exponen los criterios cuantificables y su modo de revisión, tras la tabla se expondrá la manera de determinar el grado de consecución en el apartado resultados:

Criterio	Si	No	Observación
Revisión por la dirección			
¿Coordinador y equipo se han designado correctamente?	✓		
¿Se ha seguido alguna norma?		✓	A priori, no han seguido ningún estándar, tampoco lo han indicado expresamente.
Competencia y toma de conciencia			
¿Se han comunicado los objetivos responsabilidades y fechas a los participantes?	✓		No existen fechas concretas para conocer el avance del proyecto
¿Se han comunicado nombramientos?	✓		
Determinación del alcance de los sistemas de gestión de calidad y de gestión de la seguridad			
¿Existe un documento de alcance?	✓		
Comprensión de la organización y su contexto			
¿Existe constitución de grupo?		✓	No parece haber un documento para la constitución del grupo, ni firmas, ni elementos que indiquen la

			formación del equipo
Requisitos legales y otros requisitos			
¿Existe opción de aceptar Términos?		✓	Indican que no almacenan ningún dato de terceros, por tanto podría ser prescindible
¿Se contemplan requisitos legales de seguridad sin afectar el rendimiento?	✓		Se aseguran de no almacenar datos de sus usuarios
¿Existe análisis de requisitos legales?	✓		
Definición de objetivos de calidad y seguridad a conseguir y definición del programa de gestión de calidad y seguridad			
¿Existen Objetivos documentados?	✓		
¿la planificación del proyecto es realista ?	✓		Aunque vuelvo a incidir en que no existen fechas concretas.
Comunicación			
¿Existen actas de reunión?		✓	No se indica en qué momento han tenido lugar las reuniones que hayan podido realizar, ni donde han sido realizadas.
¿Se notifican eventos a los participantes?		✓	Al menos no de manera formal.
¿La información del proyecto es accesible?	✓		
Información documentada del SGC			

y del SGSI			
¿La documentación es consistente?	✓		
Planificación y Control Operacional			
¿Se han respetado fechas?	✓		al menos en la planificación temporal, se indica un esquema claro y conciso de la dirección que debe tomar el proyecto
¿Se han recogido estimaciones y tiempos reales?		✓	En la documentación se habla de horas, pero no hay fechas concretas ni límites exactos. No se deja claro si se han cumplido
¿Se han rellenado los apartados: introducción, análisis de alternativas, objetivos, alcance, gestión de riesgos, planificación temporal, evaluación económica y conclusión?		✓	Se han rellenado todos los apartados a excepción de evaluación económica y conclusiones
¿Se han establecido las tecnologías a utilizar?	✓		
Seguimiento, medición, análisis y evaluación			
¿Existe captura de requisitos?		✓	
¿Análisis de alternativas y elección?	✓		
¿Se ha diseñado UML?	✓		

¿Son cuantificables y concretos los requisitos?		✓	
¿Existen casos de uso?		✓	
¿Existen prototipos de interfaces ?		✓	No existe un prototipo de interfaces, aunque sí que existe un prototipo inicial del proyecto sobre el papel
¿El diseño cumple los requisitos?		✓	Puesto que no hay análisis de requisitos, este punto no es comprobable.
Evaluación del cumplimiento			
¿Se ha contemplado la evaluación en el alcance?		✓	
¿Se han analizado alternativas?	✓		
Auditoria del SGC y SGSI			
¿Existe sistema de control de versiones?	✓		
¿Existe sistema de control documental?	✓		Se realiza a través de Google Drive. Podrían utilizarse herramientas más precisas (Wikis p.e)
Mejora continua			
¿Se han registrado inconformidades?		✓	
¿Existe un plan ante el riesgo?	✓		

¿Existe responsable de dicho plan?		✓	
No conformidad y acción correctiva			
¿Se han evaluado riesgos?	✓		
¿Existe registro de incidencias?	✓		
Certificación del SGSI y SGC			
¿Se han usado estándares?		✓	
¿Se han establecido al menos dos medidas de seguridad?	✓		
¿Se ha programado orientado a objetos?	✓		
¿El sistema sigue MVC?		✓	Desde la vista se accede directamente a clases del modelo, no hay observador observable.
¿Se ha usado patrones de diseño?	✓		Singleton entre otros, aunque mal implementado.
¿La app es fácil de usar?	✓		Contiene un manual de usuario explicativo.
Aplicar acciones correctivas			

¿Existen plan de pruebas?	✓		
¿Existen las pruebas y son satisfactorias?	✓		
¿Se han hecho pruebas sobre todos los requisitos?	✓		
Revisión interna del SGSI y SGC			
¿Existe revisión como tarea?		✓	Sí que existe una tarea para corrección de errores.
¿Se ha basado en prototipos?	✓		
¿Se ha planificado la revisión?		✓	
Recursos			
¿ la estructura de la organización es horizontal?		✓	No hay una estructura muy definida en el grupo
¿Todos los miembros tienen una responsabilidad definida?	✓		Así está reflejado en el documento de tareas

Resultados

A continuación se ofrece un compendio de resultados para facilitar la lectura de la tabla expuesta anteriormente;

Criterio	puntos obtenidos	puntos total	puntos ACC	puntos ACC total
Revisión por la dirección	**1**	**2**	**1**	**2**
Competencia y toma de conciencia	2	2	3	4
Determinación del alcance de los sistemas de gestión de calidad y de gestión de la seguridad	1	1	4	5
Comprensión de la organización y su contexto	0	1	4	6
Requisitos legales y otros requisitos	2	3	6	9
Definición de objetivos de calidad y seguridad a conseguir y definición del programa de gestión de calidad y seguridad	2	2	8	11
Comunicación	1	3	9	14
Información documentada del SGC y del SGSI	1	1	10	15
Planificación y Control Operacional	2	4	12	19
Seguimiento, medición, análisis y evaluación	2	7	14	26
Evaluación del cumplimiento	1	2	15	28
Auditoria del SGC y SGSI	2	2	17	30
Mejora continua	1	3	18	33
No conformidad y acción correctiva	2	2	20	35
Certificación del SGSI y SGC	4	6	24	41
Aplicar acciones correctivas	3	3	27	44
Revisión interna del SGSI y SGC	1	3	28	47
Recursos	1	2	29	49

Para entender los resultados consideramos los puntos acumulados obtenidos en las distintas componentes y los contrastamos con los puntos totales obtenibles proponiendo como corte un 6 para garantizar la excelencia exigida por las normas, es decir, subimos la nota de corte mínima para garantizar la calidad.

Por tanto el resultado de la auditoría de calidad y seguridad de la información es un 6 y se considera evidencia considerable para certificar satisfactoriamente en trabajo en cuanto a la norma expuesta anteriormente y según los criterios de auditoría explicitados, y nos como entidad procuradora, competente, y certificada acreditamos que Snake SL posee procedimientos y procesos suficientes en su organización para garantizar trabajos de calidad y competente en la seguridad de la información.

en Bilbao , 7 mayo 2019

Acreditan:

Sr Ingeniero Edgar Andrés
Nº colegiado XXXXXXXXXXXXXX

Sr Ingeniero Iván Álvarez
Nº colegiado XXXXXXXXXXXXXX

Sra Ingeniero Andrea Siles
Nº colegiado XXXXXXXXXXXXXX

conclusión

Como resultado de la revisión, existen algunos fallos y ausencias de apartados o documentos, si bien el trabajo no ha sido perfecto, está bastante completo y cumple con una amplia mayoría de requisitos., y como resumen general de la auditoría, creemos que es un buen trabajo y ha logrado por tanto nuestra certificación.

En cuanto al aspecto legal, existe documentación necesaria para garantizar el cumplimiento de la ley vigente y se aseguran de que su aplicación no entre en conflicto con ésta, además dada la índole de la aplicación creemos que se toman medidas de seguridad de la información suficientes.

Como acciones a mejorar, cabría destacar una mayor definición de las tareas a repartir entre los miembros, así como una jerarquía de trabajo, donde quede claro el máximo responsable y director del grupo, una planificación temporal más intuitiva para el cliente, donde pueda ver en fechas concretas como avanza el proyecto que espera.

Como broche comentamos el carácter competitivo de la actividad y recordamos la necesidad de mejora continua que esto acarrea por lo que estas recomendaciones que ofrecemos deben ser tomadas como estratégicas para poder garantizar la sostenibilidad del método de trabajo a largo plazo y poder así perpetuar la excelencia.

Felicidades desde el grupo de Auditoría, Bilbao 7 mayo 2019

Edgar Andrés
Andrea Siles
Iván Álvarez

Bibliografía

- Web seguridad y continuidad
  https://www.seguridadycontinuidad.com/que-es-iso-27001-resumen-de-la-norma/

- Web EAE Bussines school
  https://retos-operaciones-logistica.eae.es/iso-9001-resumen-y-principales-beneficios/

- Manual de gestión integrada (2017). Edgar Andrés,Eneko Gómez,Unai Martín
  https://github.com/EdgarAndresSantamaria/Gestion/blob/master/Manual%20de%20gesti%C3%B3n%20integrada.pdf

- Implantación de un SGA según ISO 14001 (2017), David Fernández ,
  https://github.com/EdgarAndresSantamaria/trabajosAPI/blob/master/Auditoria/Implantacion_de_un_SGA_David_Fernandez.pdf

- UNE-ISO/IEC 27001, UNE-EN ISO 9001