LISTA DE PROCEDIMIENTOS ISO 27001:2022

www.edirama.it

PROC-07-1 - Procedimiento de desarrollo de habilidades en seguridad de la información.docx
PROC-07-3 - Procedimiento de control de la información documentada.docx
PROC-09-2 - Procedimiento de auditoría interna.docx
PROC-09-4 - Procedimiento de revisión por la dirección.docx
PROC-10-1 - Procedimiento de gestión de no conformidades.docx
PROC-A05-10-4 - Procedimiento de gestión de Asset.docx
PROC-A05-10-5 - Procedimientos para la gestión de dispositivos extraviados o robados.docx
PROC-A05-12-1 - Procedimiento de clasificación de la información.docx
PROC-A05-13-1 - Procedimiento de etiquetado de información.docx
PROC-A05-14-1 - Procedimiento de transferencia de información.docx
PROC-A05-21-1 - Procedimiento de evaluación de proveedores.docx
PROC-A05-25-1 - Procedimiento de gestión de eventos de seguridad de la información.docx
PROC-A05-26-1 - Procedimiento de respuesta a incidentes de seguridad de la información.docx
PROC-A05-30-3 - Procedimiento de respuesta a incidentes de continuidad de ITC.docx
PROC-A05-31-1 - Procedimiento de gestión de requisitos legales y contractuales.docx
PROC-A05-34-2 - Procedimiento de notificación de violación de datos personales.docx
PROC-A06-1-1 - Procedimiento de selección de empleados.docx
PROC-A06-8-1 - Procedimiento de reporte de eventos de seguridad de la información.docx
PROC-A07-10-1 - Procedimiento de gestión de medios extraíbles.docx
PROC-A07-10-2 - Procedimiento de transferencia de medios físicos.docx
PROC-A07-14-1 – Procedimiento eliminación de dispositivos.docx
PROC-A07-3-1 - Procedimiento de acceso al centro de datos.docx
PROC-A07-6-1 - Procedimiento de trabajo en áreas seguras.docx
PROC-A07-9-1 - Procedimiento de retiro de activos fuera del sitio.docx
PROC-A08-8-2 - Procedimiento de evaluación de vulnerabilidad técnica.docx

EJEMPLO DEL PROCEDIMIENTO DE REVISIÓN DE LA GESTIÓN DEL SGSI ISO 27001:2022

Procedimiento de revisión por la dirección SGSI ISO 27001:2022

Índice

1 Introducción

El propósito de este documento es definir el procedimiento para realizar revisiones de gestión dentro del sistema de gestión operado por [Nombre de la empresa] de acuerdo con el estándar de seguridad de la información ISO/IEC 27001.

Las revisiones de gestión son una parte clave del sistema de gestión, ya que brindan una oportunidad regular para garantizar que se alcancen los objetivos y que las métricas se encuentren dentro de límites aceptables. También actúan como desencadenantes de acciones correctivas y como un fuerte motor de mejora dentro del SGSI.

2 Revisión de la gestión

2.1 Programación

el primer día hábil del trimestre o tan pronto como sea posible.

2.2 Participantes

La revisión de la gestión estará presidida por el Director Ejecutivo o un reemplazo designado. Los participantes adicionales normalmente serán los siguientes:

- Director de Operaciones (COO)
- Director Financiero (CFO)
- Oficial de Privacidad
- Responsable de la seguridad de la información

Las ausencias deben notificarse al menos una semana antes de la reunión programada y, cuando sea posible, debe designarse un reemplazo para que asista. Es posible que se invite a otros participantes a debatir puntos específicos del orden del día.

Todas las reuniones serán registradas en actas.

2.3 Formato

Se utilizará un formulario estándar para la revisión por la dirección. Este formulario se actualizará siempre que sea necesario cambiar el contenido de la revisión de la dirección, como agregar más temas de revisión. En la mayoría de los casos, la forma de la revisión anterior

puede utilizarse como punto de partida, siempre que se hayan incorporado cambios en el contenido.

Las actas de las reuniones deben nombrarse en el formato "Revisión de la gerencia [fecha]" y almacenarse como un documento de Word (.docx) en la carpeta [ubicación del archivo de estado] .

2.4 Clasificación

El contenido y el informe de la revisión por la dirección se tratarán como Confidenciales como parte de la definición del esquema de clasificación de la información que se utiliza en [Nombre de la empresa] . Esto significa que se debe tener el debido cuidado para proteger la confidencialidad, integridad y disponibilidad de los documentos. No deben compartirse con terceros sin un acuerdo de confidencialidad vigente.

2.5 Preparación para la revisión

Las siguientes acciones deben ser tomadas por el presidente (o el reemplazo designado) en preparación para la revisión por la dirección:

1. Invitar elementos adicionales de la agenda para la reunión
2. Asegúrese de que la persona adecuada actualice la información de apoyo necesaria para la reunión, que esté disponible y que se distribuya a todos los asistentes, lo que incluye:
    - Informes de auditoría interna y externa
    - Informes de evaluación de riesgos y planes de tratamiento
    - Informes de seguimiento y medición
    - Registro de acciones de mejora continua
    - Objetivos de seguridad de la información
    - Documentación del SGSI nueva o actualizada, p. políticas
3. Distribuir la agenda de la reunión y las actas de la revisión de la gestión del trimestre anterior
4. Asegúrese de que los recursos necesarios, como la sala de reuniones, el proyector y el encargado de tomar actas designado, estén disponibles

2.6 Áreas examinadas

Las áreas cubiertas por la revisión de la dirección pueden cambiar con el tiempo a medida que cambian los requisitos comerciales. A la fecha de este procedimiento, se incluyen las siguientes áreas:

Árbitro	Artículo	Descripción
1	Acciones de la revisión anterior	Indique si las acciones se han completado o no y, en caso contrario, cuáles son los próximos pasos
2	Cambios relevantes en el sistema de gestión	Cualquier cambio interno o externo significativo que se haya producido desde la última revisión que pueda tener un impacto en el sistema de gestión y, por lo tanto, deba tenerse en cuenta.
3	Cambios en las necesidades y expectativas de las partes interesadas	Para aquellas partes interesadas que son relevantes para el SGSI, si sus puntos de vista sobre lo que el SGSI debe ofrecer han cambiado de alguna manera
4	No conformidades y acciones correctivas	Estado de las actuaciones planteadas por auditorías internas y externas anteriores
5	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...
6	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...
7	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...
8	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...
9	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...
10	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...
11	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...
12	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...

13	v	Acciones registradas durante esta revisión, con la persona responsable y la fecha límite
14	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...

Tabla 1: Áreas examinadas

Las acciones registradas se rastrearán hasta su finalización como parte del proceso de revisión de la gestión.

3 Revisión anual de la gestión

3.1 Programación

al comienzo del ejercicio, junto con la replanificación de los objetivos comerciales para el año siguiente.

3. 2 participantes

Las revisiones anuales de gestión estarán presididas por el Director Ejecutivo o un suplente designado. Los participantes adicionales normalmente serán los siguientes:

- Director de operaciones (COO)
- Director financiero (CFO)
- Director de información (CIO)
- Director de privacidad (CPO)
- gerente de seguridad de la información
- Gerentes relevantes de la empresa, si corresponde

Se debe presentar una disculpa al menos una semana antes de la reunión programada y, cuando sea posible, se debe designar a un reemplazo para que asista. Es posible que se invite a otros participantes a debatir puntos específicos del orden del día.

Todas las reuniones serán registradas en actas.

3.3 Formato

Se utilizará una agenda estándar (como se define en 3.4 a continuación) para la revisión de gestión anual y se actualizará cada vez que el contenido de la revisión de gestión deba cambiar, por ejemplo, para agregar más temas de revisión.

Los registros deben nombrarse en el formato "Revisión de gestión anual [fecha]" y almacenarse como un documento de Word (.docx) en la carpeta [indique la ubicación del archivo] .

3.4 Clasificación

El contenido de las actas anuales de revisión de la gestión se tratará como Confidencial como parte de la definición del esquema de clasificación de la información en uso dentro de [Nombre de la empresa] . Esto significa que se debe tener el debido cuidado para proteger la confidencialidad, integridad y disponibilidad de los documentos. No deben compartirse con terceros sin un acuerdo de confidencialidad vigente.

3.5 Preparación de la revisión anual

Las siguientes acciones deben ser tomadas por el presidente (o el reemplazo designado) en preparación para la revisión de gestión anual (además de las de la revisión trimestral):

- Asegúrese de que la persona adecuada actualice la información de apoyo necesaria para la reunión, que esté disponible y que se distribuya a todos los asistentes, lo que incluye:
    - Detalles de los cambios recomendados en la documentación del SGSI
    - Declaración actual de aplicabilidad
    - Detalles de los auditores actuales

3.6 Áreas examinadas

En esta revisión, además de la agenda trimestral habitual , se examinarán las siguientes áreas:

Árbitro	Actividad	Descripción
1	Revisión de la documentación del SGSI	Un informe de revisión de todos los documentos dentro del sistema de gestión para cambios de contenido, como actualizaciones y eliminación de información obsoleta, es decir, todas las políticas, procedimientos y archivos de información.
2	Revisión de objetivos	Se fijarán nuevos objetivos anuales para los próximos 12 meses
3	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...

4	…… VERSIÓN COMPLETA DISPONIBLE...	…… VERSIÓN COMPLETA DISPONIBLE...

Tabla 2: Áreas adicionales examinadas durante la revisión anual

Se registrará la revisión anual y se seguirán las acciones hasta su finalización.