

MN_EMO

The cover features a complex geometric design. A large white triangle points downwards from the top left. The background is a collage of green and grey tones, including a cityscape on the right and abstract gear-like patterns at the bottom. The text 'MN_EMO' is prominently displayed in the upper left, with the 'E' in a green subscript. A horizontal line with a green arrow points to the right, passing through the center of the page.

Módulo 4
Soporte

Contenido

Introducción	3
Objetivos	3
Recursos	3
Competencia.....	4
Concienciación.....	5
Comunicación	6
Establecimiento de los mecanismos internos de comunicación y de información.....	6
Qué se comunica:.....	7
Cuándo se comunica:.....	7
Con quién comunicarse:.....	8
Cómo comunicarse:	9
Establecimiento de los mecanismos externos de comunicación y de información	11
Qué se comunica:.....	12
Cuándo se comunica:.....	12
Con quién comunicarse:.....	13
Cómo comunicarse:	14
Información documentada	16
Creación y actualización de la documentación	16
Control documental	16
Listado de Documentos	17

Introducción

Cada día más, se hace necesario en las organizaciones el contar con un sistema de protección de la información, que nos ayude a identificar las amenazas a las que estamos expuestos y poder controlarlas.

La implantación de un SGSI (Sistema de Gestión de Seguridad de la Información) nos va a permitir asegurar la protección de los activos de información de nuestro negocio, mediante la reducción de riesgos y costos, y maximización de las oportunidades de negocio.

Un elemento clave para la implantación y operación de un SGSI, es dotarle de los recursos adecuados, sin ello, una de las piezas prioritaria fallará e impedirá al SGSI cumplir con los objetivos encomendados. Entendemos como recursos del SGSI a las personas, formación y competencia, concienciación, necesidades de comunicación y el control sobre la información documentada.

Objetivos

En este módulo vamos a conocer cuáles son los requerimientos de ISO/IEC 27001:2022 respecto a la dotación de recursos, incluyendo la competencia del personal, la concienciación no solo de los empleados sino también de aquellas personas que trabajan para la organización, y por último también revisaremos un punto importante de la norma como es la comunicación, tanto interna como externa.

Recursos

La organización debe determinar y proporcionar los recursos necesarios para mejorar el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información. Uno de los aspectos más importantes que la dirección debe perseguir es proporcionar dichos recursos teniendo en cuenta que en cada

una de las etapas se requerirán unos recursos concretos. Para ello se recogerá en la política de Seguridad de la Información dicho compromiso.

Para cada responsabilidad y función en el SGSI se debería tener en consideración lo siguiente:

- Las personas, las habilidades, la experiencia y las competencias.
- Los recursos necesarios para cada etapa del proceso de gestión del riesgo.
- Los procesos de la organización, los métodos y las herramientas a utilizar para gestionar el riesgo.
- Los procesos y procedimientos documentados.
- Los sistemas de gestión de la información y del conocimiento.
- Los programas de formación.

El presupuesto de la organización debería reflejar la planificación y compromiso de estos recursos.

Competencia

La organización debe garantizar que todo el personal al que se le hayan asignado responsabilidades dentro del SGSI sea competente para llevar a cabo sus tareas. Para ello deberá:

- Determinar las competencias necesarias.
- Asegurarse de que estas personas son competentes en la base en la educación, la formación o la experiencia.
- En su caso, tomar medidas para adquirir las competencias necesarias, y evaluar la eficacia de las medidas adoptadas.
- Retener la información documentada apropiada como prueba de competencia.

Las acciones aplicables pueden incluir, por ejemplo, la oferta para formación, tutorías, la reasignación de los empleados actuales, o la contratación de personas competentes.

El alumno deberá consultar en la plataforma el recurso: Roles Responsabilidades y Competencias_v2Perfiles.pdf, donde encontrará la relación de todos los roles que intervienen en la implantación de un SGSI con sus respectivos roles, responsabilidades y requisitos de competencias con las que deben contar.

Concienciación


La concienciación referida a la Seguridad de la Información es un pilar fundamental de la gestión de la seguridad. Las personas (internas o externas) que realizan trabajos bajo el control de la organización deberán tener en cuenta:

- Políticas y Normativas de la organización en seguridad de la información.
- Curso de concienciación en protección de datos.
- Sensibilización en seguridad de la información.
- Curso de concienciación de phishing y malware
- Entre otros.

Tanto la concienciación como la formación deben ser registradas y medidas para poder evaluar su eficacia. Se deben crear y mantener los registros para proporcionar las evidencias de dicha formación.

En el caso de personal externo, se deben establecer los mecanismos para implantar y medir el control, de acuerdo con el contrato existente y a la legislación laboral actual.

El alumno debe consultar el siguiente recurso en la plataforma: Plan de Formación, donde encontrará un modelo para documentar el plan de formación de una organización.



A continuación, se muestra un ejemplo para Autos Europa:

PERSONA	ROL	CURSO	OBJETIVO DE LA ACCIÓN FORMATIVA	HECHO	FECHA PREVISTA	FECHA REALIZACIÓN
Luis Arturo Díaz	Administrador ERP	Política de Seguridad de la Información	Dar a conocer la Política de Seguridad de Autos Europa		Marzo 10 de 2017	Marzo 10 de 2017

Los cursos pueden ser Online o presenciales, algunos ejemplos de cursos de concienciación pueden ser:

- Curso de concienciación en protección de datos.
- Sensibilización en seguridad de la información.
- Curso de concienciación de phishing.
- Entre otros.

Comunicación

La organización debe determinar la necesidad de las comunicaciones internas y externas relacionadas con el Sistema de Gestión de Seguridad de la Información, incluyendo:

- Qué comunicar.
- Cuándo comunicar.
- A quién comunicar.
- Quién debe comunicar.
- Cómo se llevará a cabo la comunicación.

Establecimiento de los mecanismos internos de comunicación y de información

La organización debería establecer mecanismos internos de comunicación y de información con objeto de apoyar y fomentar la obligación de rendir cuentas y la propiedad del riesgo. Estos mecanismos deberían garantizar:

- La comunicación adecuada de los componentes clave del marco de trabajo de la gestión del riesgo, así como de todas las modificaciones posteriores.

- La existencia de informes internos adecuados sobre el marco de trabajo, su eficacia y sus resultados.
- La disponibilidad de información apropiada obtenida de la aplicación de la gestión del riesgo en los niveles y tiempos apropiados.
- La existencia de procesos para realizar consultas con las partes interesadas.

Cuando corresponda, estos mecanismos deberían incluir procesos para consolidar la información relativa al riesgo procedente de fuentes diferentes, y puede ser necesario considerar la sensibilidad de la información.

Qué se comunica:

Se comunicará cualquier información que guarde relación con el SGSI.

- Sistema de Gestión de Seguridad de la Información:
 - Comunicación de incidentes de seguridad.
 - Comunicación de No Conformidades y de Acciones correctivas.
 - Comunicación de Acciones de Mejora (propuesta, realización, etc.).
 - Comunicación de datos de cumplimiento de objetivos/métricas.
 - Comunicación de las partes interesadas, y de los recursos necesarios para que los procesos de negocio operen como normalidad.

Cuándo se comunica:

Se realizarán comunicaciones siempre que:

- Se requiera la intervención de cualquier otra parte en cualquier tarea involucrada dentro del SGSI.
- Sea necesario realizar la comunicación lo antes posible para evitar un daño mayor (incidentes).
- Sea necesario informar a partes involucradas dentro de un proceso de cambio, acción correctiva o acción de mejora.

- Sea necesario obtener información sobre recursos necesarios, activos involucrados, valoraciones, tiempos de respuesta, etc.

Con quién comunicarse:

En el ámbito interno, las comunicaciones se realizan principalmente con otros trabajadores.

1) Comunicación horizontal, entre Departamentos / Áreas: En este caso, las vías de comunicación utilizadas pueden ser:

- Comunicaciones a través del correo electrónico o cualquier otro método de transmisión digital.
- Comunicados internos por escrito.
- Comunicación verbal.
- La propia documentación del Sistema de Gestión.

2) Comunicación vertical, entre los diferentes Unidades / Áreas /Departamentos y Dirección. En este caso, las vías de comunicación utilizadas son:

- Reuniones periódicas de Técnicos / Jefes de Área / Directores de Departamento con Dirección.
- Comunicación verbal.
- Comunicados internos por escrito.
- La propia documentación del Sistema de Gestión.

3) Comunicación de Incidentes al responsable del SGSI:

En el caso de producirse un incidente, el mismo se comunicará tal y como está descrito en los documentos de la organización.

4) Comunicación con la dirección:

La comunicación con la Dirección se realizará principalmente de forma presencial (verbal), o bien a través de videoconferencia o vía telefónica si alguna de las partes se encuentra

fuera de las instalaciones. También se utilizará el correo electrónico para el traspaso de ficheros, y comunicaciones vía mail.

Cómo comunicarse:

Los principales recursos implantados para garantizar la comunicación son los siguientes:

- Correo electrónico corporativo: es un sistema accesible desde las propias instalaciones de la organización, desde el exterior a través de Internet, y a través de los smartphones proporcionados por la organización.
- Dispositivos móviles smartphones: son dispositivos que disponen de conexión con el correo corporativo a través de una línea de datos móviles o de una red wifi, y que también permiten la comunicación mediante la red UMTS.
- Equipamiento informático: los equipos informáticos disponen de cliente de correo electrónico permitiendo el envío de comunicados vía correo electrónico, y de suite ofimática, permitiendo elaborar comunicados por escrito.
- Impresoras multifunción con escáner: facilitan las comunicaciones por escrito, permitiendo escanear comunicados para enviarlos por correo electrónico, o bien imprimir comunicados que necesitan realizarse en formato papel.
- Terminales Voz IP: Estos dispositivos se encuentran ubicados dentro de la propia organización, y permiten la comunicación directa entre las personas de la organización, realizando llamadas contra otro terminal Voz IP o contra terminales móviles.
- Mensajería instantánea corporativa: programa corporativo instalado en los equipos de la organización, que permite la comunicación por chat con el resto del personal. Este programa también permite el traspaso de ficheros, así como realizar sesiones de videoconferencia.
- Tablón de anuncios: Mediante un tablón de anuncios donde la organización se comunica con sus empleados, facilitando noticias de interés para los

empleados, en algunos casos son los propios empleados los que colocan artículos de interés.

- Páginas Web: Mediante esta herramienta, la organización dispone de un medio de comunicarse con todas las personas interesadas tanto internas como externas, haciendo llegar los mensajes institucionales sobre determinada situación y/o incidente.

En todo caso, la Organización facilita los medios necesarios para que cualquiera de sus integrantes pueda comunicar sus necesidades y propuestas de mejora.

Las comunicaciones internas presentadas al Comité de Dirección serán evaluadas en el mismo, comunicándose las resoluciones adoptadas.

Tabla Global:

Qué	Quién realiza la comunicación	A quién	Cuándo	Medio	Proceso/Procedimiento
Política de Seguridad de la Información	Dirección (a través de RRHH)	Empleados Subcontratistas	Aprobación Aprobación	Email/Intranet E-mail	
	Responsable SGSI	Comité Dirección	Antes de aprobarla	Presencial / Comité	
	XXXXXXX	Proveedores	Aprobación	Web	
	XXXXXXX	Clientes	Aprobación	Web	
	XXXXXXX	Compañías de Seguros	Cuando solicitan	E-mail	
	Responsable SGSI	Otros	Cuando solicitan y si es aprobado	E-mail o Mostrar presencialmente	

Qué	Quién realiza la comunicación	A quién	Cuándo	Medio	Proceso/Procedimiento
Incidentes de seguridad de la información	Empleados Subcontratistas	Responsable SGSI	Cuando ocurre	XXXXXX	
	Responsable SGSI	Comité Dirección	Cuando ocurre Resumen	Comité Dirección	
	Responsable SGSI	Proveedores	Cuando ocurre	E-Mail / Teléfono / Presencial	
	Proveedores	XXXXXXX	Cuando ocurre	E-Mail / Teléfono / Presencial	
	Responsable SGSI	Clientes	Cuando ocurre	E-Mail / Teléfono / Presencial	
	Cliente	Responsable SGSI	Cuando ocurre	E-Mail / Teléfono / Presencial	
	Dirección	Compañías de Seguros	Cuando ocurre	E-Mail / Carta o Escrito certificado	
	Responsable SGSI	Estado/Gobierno (AEPD)	Cuando ocurre	E-Mail / Presencial / Carta certificada	
	Dirección	Estado/Gobierno (Cuerpos y fuerzas de seguridad)	En función de la magnitud del incidente	Presencial - Denuncia	

Qué	Quién realiza la comunicación	A quién	Cuándo	Medio	Proceso/Procedimiento
Resultados medición (métricas)	Empleados internos	Responsable SGSI	Mensual	E-Mail Presencial	
Resultados mediciones e indicadores	Responsable SGSI	Comité Dirección	Mensual	Presencial E-mail	
Cambios (incluye documentación)	Responsable SGSI	Empleados Subcontratistas	Si están involucrados	E-mail Presencial	
Propuesta de cambio	Responsable SGSI	Comité Dirección	Comité	Presencial E-mail	
Cambios (incluye documentación)	Responsable SGSI	Proveedores	Si están involucrados	Presencial E-mail	
Cambios (incluye documentación)	Responsable SGSI	Clientes	Si están involucrados	Presencial E-mail	
Programa y planes auditorías	Responsable SGSI	Comité Dirección	Comité	Comité	
Resultados auditorías	Responsable SGSI	Comité Dirección	Comité	Comité	
Resultados auditorías	Responsable SGSI	Clientes	Si están acordado o lo solicitan	E-mail Presencial	
Resultados evaluación de riesgos	Responsable SGSI	Comité Dirección	Comité	E-mail Presencial	
Resultados evaluación de riesgos	Responsable SGSI	Propietarios de Riesgo	Comité Reunión	E-mail Presencial	
				seguimiento / E-mail	
	Personal interno Personal externo	Responsable SGSI	Cuando se detecta	Presencial E-mail	
	Cliente	XXXXXXX	Seguimiento servicio (queja)	E-mail Presencial	

Establecimiento de los mecanismos externos de comunicación y de información

La organización debería desarrollar e implementar un plan para comunicarse con las partes interesadas externas. Este plan debería implicar:

- La participación de las partes interesadas externas apropiadas, asegurándose un intercambio eficaz de información.
- El establecimiento de informes externos conformes con los requisitos legales, reglamentarios y de gobierno de la organización.
- La disponibilidad de retroalimentación y de informes sobre comunicación y consulta.
- La utilización de comunicaciones para generar confianza en la organización.

La comunicación con las partes interesadas en caso de crisis o contingencias. La Dirección proporciona los recursos necesarios para asegurar el establecimiento de los procesos de comunicación apropiados en el seno de la Organización. Las actividades de comunicación

pueden desarrollarse a través de diferentes vías, en función de los participantes de dicha comunicación.

Qué se comunica:


Se comunicará cualquier información que guarde relación con el Sistema de Gestión de Seguridad de la Información en alguno de los contextos externos.

A continuación, se identifica la información a comunicar:

- Incidencias con proveedores, que pudieran afectar a la seguridad de la información.
- Cambios del Gobierno que pudieran afectar al negocio o Pérdida de confianza por parte de los Inversores.
- Problemas con los requisitos, funcionalidad o calidad de los servicios prestados a clientes.
- Problemas de imagen de la organización o Cambios en los que está involucrado personal externo

Cuándo se comunica:

Se realizarán comunicaciones siempre que:

- Se requiera la intervención de cualquier otra parte en cualquier tarea externa involucrada dentro del SGSI.
 - Sea necesario realizar la comunicación lo antes posible para evitar un daño mayor (incidentes).
 - Sea necesario informar a partes externas involucradas dentro de un proceso de cambio, acción correctiva o acción de mejora.
 - Sea necesario informar sobre problemas con los servicios prestados al cliente.
 - Sea necesario informar sobre problemas relacionados con proveedores.
- 

Con quién comunicarse:

En el ámbito externo, las comunicaciones se realizan principalmente con otras organizaciones.

1) Comunicación con clientes.

La comunicación con los clientes se realizará a través de distintas vías:

- Mediante la web pública de la organización.
- Mediante correo electrónico u otro medio de comunicación digital.
- Mediante reuniones periódicas.
- Mediante interlocutores autorizados que lo sean debido a sus tareas habituales y a los niveles que se consideren adecuados.

2) Comunicación con partners y proveedores.

- Mediante la web pública de la organización.
- Mediante correo electrónico u otro medio de comunicación digital.
- Mediante reuniones periódicas.
- Mediante interlocutores autorizados que lo sean debido a sus tareas habituales y a los niveles que se consideren adecuados.

Comunicación de Incidentes al responsable del SGSI, en los que haya partes externas involucradas:

En el caso de producirse un incidente, el mismo se comunicará tal y como está descrito en los documentos de la organización.

3) Comunicación con la comunidad local (incluyendo autoridades) y otras partes interesadas (incluyendo medios de comunicación).

Únicamente la dirección y en quienes deleguen debido a la naturaleza de la comunicación pueden establecer estas comunicaciones. En concreto:

- Comunidad local (incluyendo autoridades): por norma general las áreas de RRHH y de EHS&S serán los interlocutores naturales.
- Medios de comunicación: por norma general el Consejero Delegado y los miembros del Comité de Dirección en su ausencia.

El medio de comunicación también dependerá de la naturaleza de la comunicación, siendo los medios habituales el teléfono o los encuentros presenciales.

Cómo comunicarse:

Los principales recursos implantados para garantizar la comunicación son los siguientes:

- Correo electrónico corporativo: es un sistema accesible desde las propias instalaciones de la organización, desde el exterior a través de Internet, y a través de los smartphones proporcionados por la organización.
- Dispositivos móviles smartphones: son dispositivos que disponen de conexión con el correo corporativo a través de una línea de datos móviles o de una red wifi, y que también permiten la comunicación mediante la red UMTS.
- Equipamiento informático: los equipos informáticos disponen de cliente de correo electrónico permitiendo el envío de comunicados vía correo electrónico, y de suite ofimática, permitiendo elaborar comunicados por escrito.
- Impresoras multifunción con escáner: facilitan las comunicaciones por escrito, permitiendo escanear comunicados para enviarlos por correo electrónico, o bien imprimir comunicados que necesitan realizarse en formato papel.
- Faxes/Buofax: pese a que actualmente es una tecnología en desuso, en algunos casos puede utilizarse el fax para enviar documentos de forma rápida y sencilla, ya sea mediante una línea de fax específica, o a través del servicio de buofax que ofrece la web de correos.
- Terminales Voz IP: Estos dispositivos se encuentran ubicados dentro de la propia organización, y permiten realizar llamadas al exterior.

- Páginas Web: Mediante esta herramienta, la organización dispone de un medio de comunicarse con todas las personas interesadas tanto internas como externas, haciendo llegar los mensajes institucionales sobre determinada situación y/o incidente

Tabla Global:

Parte interesada	Qué	Cuándo	Medio
Proveedores	Problemas con el servicio prestado	En cuanto ocurran	Correo electrónico Vía Telefónica
	Sospecha de espionaje industrial o de competencia desleal	En cuanto se sospeche	Vía Telefónica
	Robo de información confidencial	En cuanto se sospeche	Vía Telefónica
	Incidencias con otros proveedores	En cuanto ocurran	Correo electrónico Vía Telefónica
	Incumplimiento de la legislación aplicable propio o de otros proveedores	En cuanto se detecte	Correo electrónico Vía Telefónica
	Realización de Cambios	Cuando se proponga el cambio y se planifique su acometida	Correo electrónico Vía Telefónica

Parte interesada	Qué	Cuándo	Medio
Trabajadores internos de la organización	Sospecha de espionaje industrial o de competencia desleal	En cuanto se sospeche	Vía Telefónica
	Robo de información confidencial	En cuanto se sospeche	Vía Telefónica
	Incumplimiento de la legislación aplicable por un externo	En cuanto se detecte	Correo electrónico Vía Telefónica
	Realización de cambios	Cuando se proponga el cambio y se planifique su acometida	Correo electrónico Vía Telefónica

Parte interesada	Qué	Cuándo	Medio
Clientes	Problemas con los requisitos, funcionalidad o calidad de los servicios prestados	Cuando se detecte un problema con el servicio o producto	Correo electrónico Vía Telefónica
Gobierno	Cambios del Gobierno que pudieran afectar al negocio	Cada vez que se produzca un cambio en el Gobierno, o el Gobierno realice cambios	Boletines Oficiales Cambios en la Ley (Reforma laboral, estatuto de los trabajadores, etc.)
Inversores	Pérdida de confianza total o parcial	Cada vez que las acciones pierden valor	Correo electrónico Vía Telefónica

Información documentada

La información del Sistema de Gestión de Seguridad de la Información debe incluir:

- Información documentada requerida por la norma internacional.
- Información documentada determinada por la organización como necesaria para la efectividad del Sistema de Gestión de Seguridad de la Información.

El alcance de la información documentada para un Sistema de Gestión de Seguridad de la Información puede diferir de una organización a otra debido a:

- El tamaño de la organización y el tipo de actividades, procesos, productos y servicios.
- La complejidad de los procesos y sus interacciones.
- La competencia de las personas.

Creación y actualización de la documentación

Al crear y actualizar la información documentada de la organización debe asegurarse de:

- Identificación y descripción (por ejemplo, un título, fecha, autor, o el número de referencia).
- Formato (por ejemplo, el idioma, la versión de software, gráficos).
- Los medios de comunicación (por ejemplo, papel, electrónico).
- La revisión y aprobación de la idoneidad y suficiencia.

Control documental

Los documentos requeridos por el Sistema de Gestión de Seguridad de la Información y por esta norma internacional deben ser controlados para asegurar:

- Que están disponibles y adecuados para su uso, donde y cuando sea necesario.
- Que estén protegidos adecuadamente (por ejemplo, de la pérdida de confidencialidad, uso indebido, o la pérdida de la integridad).

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

- La distribución, acceso, recuperación y uso.
- Almacenamiento y conservación, incluyendo la preservación de la legibilidad.
- El control de cambios (control de versiones, por ejemplo).
- La retención y disposición.

El acceso implica una decisión sobre el permiso ya sea solo de ver la información documentada, o el permiso y la autoridad para ver y cambiar la información documentada, etc.

Listado de Documentos

Hay que recordar que en esta norma se ha eliminado la obligatoriedad de mantener un listado de documentos obligatorios (aunque sigue siendo altamente recomendable), aunque en el cuerpo del estándar se hace referencia a distintos requisitos documentales. Por otro lado, se elimina la separación entre documentos y registros, siendo denominados simplemente "información documentada".

Estos son los documentos (adicionalmente a los "registros") que necesita si se quiere cumplir con la norma ISO 27001:2022:

- Alcance del SGSI (cláusula 4.3), incluyendo los puntos 4.1 y 4.2.
- Los requisitos legales, reglamentarios y contractuales (cláusulas 4.2 y A5.31).
- Política y objetivos de Seguridad de la Información (cláusulas 5.2 y 6.2).
- Procesos para la evaluación de riesgos y el tratamiento de riesgos (cláusulas 6.1.2 y 6.1.3).
- Declaración de Aplicabilidad (cláusula 6.1.3 d).
- Planificación y Control Operacional (cláusula 8.1).

Tenga en cuenta que los documentos del Anexo A son obligatorios si hay riesgos que tratar, requisitos legales o contractuales, normativas internas o externas que exigirían la aplicación.

Y aquí están los registros obligatorios:

- Comunicación de la política (cláusula 5.2).
- Comunicación de responsabilidades y autoridades (cláusula 5.3).
- Planificación de acciones para el tratamiento de riesgos y oportunidades y para el logro de los objetivos (cláusulas 6.1 y 6.2).
- Los registros de capacitación, las habilidades, la experiencia y las cualificaciones (cláusula 7.2).
- Registros de concienciación (cláusula 7.3).
- Necesidades de comunicación (cláusula 7.4).
- Informe de evaluación de riesgos (cláusula 8.2).
- Los resultados del monitoreo, medición, análisis y evaluación (cláusula 9.1).
- Programa de auditoría interna: definición, implementación, mantenimiento (cláusula 9.2).
- Reporte de los resultados de las auditorías internas (apartado 9.2).
- Gestión por parte de la Dirección de la información recibida y de los resultados. (cláusula 9.3).
- Gestión de los resultados de las acciones correctivas y de las oportunidades de mejora (cláusula 10.1).

Existen numerosos documentos que podrían ser requeridos si son necesarios para garantizar la efectividad del SGSI (cláusula 7.5.1b).

- Procedimiento para control de documentos (cláusula 7.5.3).
- Controles para gestión de registros (cláusula 7.5).
- Procedimiento para auditoría interna (cláusula 9.2).
- Procedimiento para medidas correctivas (cláusula 10.1).

- Política Trae tu propio dispositivo (Bring your own device - BYOD) (control A8.1).
- Política sobre dispositivos móviles y teletrabajo (control A8.1).
- Política de clasificación de la información (controles A5.12, A5.13, y A5.10).
- Política de claves (controles A5.16, A5.18, y A5.17).
- Política de eliminación y destrucción (controles A7.10, y A7.14).
- Procedimientos para trabajo en áreas seguras (control A7.6).
- Política de pantalla y escritorio limpio (control A7.7).
- Política de gestión de cambio (control A8.32).
- Política de creación de copias de seguridad (control A8.13).
- Registro sobre actividades de los usuarios, excepciones y eventos de seguridad (control A8.15).
- Inteligencia sobre las amenazas (nuevo control A5.7).
- Seguridad de la información para el uso de servicios en la nube (nuevo control A5.23).
- Preparación de las TIC para la continuidad del negocio (nuevo control A5.30).
- Monitoreo de seguridad física (nuevo control A7.4).
- Gestión de la configuración (nuevo control A8.9).
- Eliminación de información (nuevo control A8.10).
- Enmascaramiento de datos (nuevo control A8.11).
- Prevención de la fuga de datos (nuevo control A8.12).
- Monitorización de las actividades (nuevo control A8.16).
- Filtrado de la web (nuevo control A8.23).
- Codificación segura (nuevo control A8.28).

Los documentos y registros pueden estar en cualquier formato o tipo de medio y deben asegurar que las acciones son trazables a las decisiones de la dirección y a las políticas, y asegurar que son reproducibles los resultados registrados.

La extensión de la documentación de SGSI puede diferir de una organización a otra debido al tamaño de la organización y el tipo de sus actividades, además del alcance y complejidad de los requisitos de seguridad y el sistema que está siendo gestionado.

En general, la documentación del SGSI puede ser estructurada como una pirámide de cuatro niveles, donde la política y los manuales están en la parte más alta, se descende a través de guías y procedimientos, y finalmente se obtienen instrucciones detalladas y los registros del sistema.

