Política de seguridad de la información

MAS Prevención, Servicio de Prevención, S.L.U.

Título del documento	Política de seguridad de la información
Tipo de documento	Política
Descripción	Documento que define la política de seguridad de la información en Más Prevención, Servicio de Prevención, S.L.U.
Nivel de seguridad	Público

Registro de versiones		
Descripción	**Versión**	**Fecha**
Versión inicial del documento	1.0	23/09/2021
Se añade las fechas de aprobación del documento	2.0	14/07/2022

Registro de aprobación	
Acción	**Autor**
Realiza	SOTHIS
Revisa	
Aprueba	

Control de distribución

ÍNDICE

1 Aprobación y entrada en vigor

El presente documento ha sido aprobado el día 14/07/2022, por parte de la Dirección de **Más Prevención, Servicio de Prevención, S.L.U. (SPMAS)**. Desde esta fecha, la presente Política entra en vigor hasta que se reemplace mediante la aprobación de una nueva o se invalide.

2 Objeto

SPMAS, para alcanzar sus objetivos en el normal desarrollo de su actividad, depende altamente de los sistemas TIC (Tecnologías de Información y Comunicaciones) que conforman la arquitectura tecnológica de la organización.

Estos sistemas deben ser administrados con la debida diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad, así como autenticidad y trazabilidad de la información tratada o de los servicios que se prestan.

El fin único la presente política, es **garantizar la seguridad de la información y la prestación continuada de los servicios**, actuando de manera preventiva, supervisando las actividades diarias que se desarrollan en la organización y reaccionando con celeridad y resiliencia frente a los posibles incidentes de seguridad.

Asimismo, y con el objetivo de garantizar la disponibilidad de los servicios, los **departamentos y áreas** de la organización, deben desarrollar planes de continuidad de los sistemas TIC como parte de su Plan de Continuidad de Negocio TIC y actividades de recuperación.

3 Alcance

La presente Política se aplica a todas las partes interesadas del Sistema de Gestión de Seguridad de la Información (SGSI) de SPMAS. Esta información se encuentra dispuesta de manera general en el documento **Alcance y contexto del SGSI** y de forma detallada en el documento **Partes interesadas del SGSI**.

4 Marco normativo

Esta Política se desarrolla conforme al marco normativo y legal aplicable en materia de seguridad, concretamente:

- UNE-EN ISO/IEC 27001, Tecnología de la información, Técnicas de seguridad, Sistemas de Gestión de la Seguridad de la Información, Requisitos.

- UNE-EN ISO/IEC 27002, Tecnología de la Información, Técnicas de seguridad, Código de prácticas para los controles de seguridad de la información.
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales y lo relativo a los mismos en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- En materia de protección de datos de carácter personal, SOTHIS cumple con los dispuesto en el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Asimismo, la presente política se desarrolla mediante un conjunto de documentos que forman la normativa interna del sistema integrado de gestión. Que se comprende de los siguientes ámbitos:

- Clasificación y etiquetado de la Información
- Seguridad en Explotación
- Seguridad en las Comunicaciones
- Gestión de Auditoría Interna de Seguridad
- Mejora Continua del Sistema de Gestión
- Gestión de la Seguridad en las Relaciones con Terceros
- Gestión de Activos y Soportes
- Análisis y Gestión de Riesgos
- Gestión de la Documentación del Sistema de Gestión
- Gestión de Copias de Seguridad y Restauración
- Gestión de Incidentes de Seguridad
- Gestión de Acceso Lógico de la Información
- Seguridad física y del entorno
- Adquisición, Desarrollo y Mantenimiento de Sistemas
- Gestión de la Continuidad del Servicio
- Gestión de Supervisión de Sistemas
- Firma electrónica, certificados y controles criptográficos
- Gestión de la seguridad en la relación con las personas

La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

5 Desarrollo

5.1. Organización y gestión de la seguridad de la información

5.1.1 Roles y responsabilidades

En el marco de cumplimiento la Norma ISO/IEC 27001, y a fin de conformar la estructura de responsables en materia de seguridad, se han determinado los siguientes roles principales:

- **Responsable de la Información**, representado por miembros de la dirección de la organización, como máximos responsables de la seguridad de la información.
- **Responsable de Servicio**, representado por los responsables de cada uno de los equipos operativos.
- **Responsable de Seguridad de la Información,** es el responsable de establecer y mantener las Políticas de Seguridad de la Información, estándares, directivas y procedimientos de la Organización y representado por el responsable del **Área de Sistemas y Transformación Digital**.
- **Responsable de Sistemas**, responsable de la infraestructura de sistemas y comunicaciones.
- **Responsable de Instalaciones,** representado por el **Responsable de Infraestructuras** de la organización.

Adicionalmente, la atención, revisión y auditoría de la seguridad de los sistemas será realizada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida.

Asimismo, **SPMAS** dispone de mecanismos de coordinación y resolución de conflictos, recayendo en la Dirección la responsabilidad de su gestión y toma de decisiones. El detalle de las atribuciones, roles y sus respectivas funciones, así como los procesos de están detallados en el documento **Roles y responsabilidades**.

5.1.2 Comité de seguridad de la información

A fin de conformar esta estructura, la Dirección de **SPMAS**, como responsable último de la información, designa un **Comité de Seguridad de la Información (Comité de Seguridad o Comité)**, responsable de alinear todas las actividades de carácter estratégico en materia de seguridad interna, con los requisitos de negocio de la organización.

Las actividades principales de este Comité tratan lo referente a la protección de los Sistemas de Información, la gestión de riesgos, y la supervisión, aprobación y mantenimiento del SGSI.

El Comité es el encargado de promover la seguridad en la organización, tratando cualquier desviación y/o excepción que se produzca, fomentando la participación e implicación de los usuarios, y proponiendo la asignación de roles y responsabilidades en la materia.

Asimismo, cabe destacar que el Comité de Seguridad se encuentra liderado por el **Responsable de Seguridad**, como representante y garante de que la gestión de la seguridad de la información es conforme a los requisitos aplicables, y encargado de informar a la Dirección acerca de los aspectos que conciernen a la seguridad de la información desde todas sus perspectivas.

5.2. Principios relativos a la seguridad de la información

SPMAS cumple con los principios relativos a la seguridad de la información descritos a continuación:

- La seguridad de la información es comprendida como un proceso integral donde intervienen todos los elementos técnicos, humanos, materiales y organizativos, relacionados con la protección de la información.
- En seguridad de la información se diferencian las atribuciones estratégicas de las operativas.
- Para el correcto desarrollo del SGSI se fomenta la capacitación, formación y concienciación de las personas implicadas, de acuerdo con sus funciones y responsabilidades en seguridad de la información.
- El análisis y la gestión de riesgos es parte esencial del proceso de seguridad, debiendo mantenerse actualizado de manera continua, a fin de disponer de un entorno controlado y seguro.
- Con el fin de reducir la probabilidad de ocurrencia y el impacto relativo a la materialización de las posibles amenazas de seguridad, se planifican e implementan medidas orientadas a su prevención, detección, corrección y mejora continua.
- La estrategia de protección se basa en múltiples líneas de defensa, constituidas por medidas de naturaleza organizativa, física y lógica, establecidas en un marco de mejora continua donde se evalúan y actualizan periódicamente con el objetivo de medir su eficacia.

5.3. Objetivos de seguridad

Se establecen, a continuación, los objetivos de seguridad de la información en **SPMAS**:

- Definir un marco de gobierno de seguridad de la información.
- Establecer una gestión de activos eficaz.
- Elevar el nivel de seguridad en el acceso lógico a los sistemas de información.
- Prevenir la fuga de información corporativa fuera de los límites de la organización.
- Establecer un Plan de Continuidad TIC.
- Formar y concienciar a los usuarios en materia de seguridad de la información y privacidad.

5.4. Obligaciones del personal

Todas las personas de **SPMAS** tiene la obligación de conocer y cumplir la presente Política de Seguridad de la Información y la Normativa de Seguridad que la desarrolla, así como desempeñar sus competencias con profesionalidad y ética.

Es responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados. Se establecerá un plan de formación y concienciación continua, en materia de seguridad de la información para atender a todas las personas de **SPMAS** según su grado de responsabilidad.

5.5. Terceras partes

Cuando **SPMAS** preste servicios o maneje información de terceros, se les hará participes de esta Política de Seguridad de la Información en la medida que se requiera, y se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **SPMAS** utilice servicios de terceros o ceda información a terceros, transmitirá también los requisitos de esta Política y de la Normativa de Seguridad que ataña a dichos servicios o información.)

SPMAS únicamente cederá información a terceros que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos establecidos en su Política de Seguridad. Asimismo, se establecerán procedimientos específicos de reporte y resolución de incidencias.

De manera adicional, se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en la presente Política.

Por último, se adoptarán las medidas oportunas en caso de incumplimiento de estos requerimientos, por parte de un tercero.

6 Mejora continua

La Dirección de **SPMAS** se compromete a mejorar de manera continua la seguridad de la información, a través del mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información, y de las medidas técnicas y organizativas relativas a este. Es por ello por lo que se sigue un enfoque basado en el ciclo de mejora continua conocido como **Ciclo PDCA (Plan, Do, Act, Check) o Ciclo de Deming**, el cual consiste en planificar, hacer, verificar y actuar, en relación con el desempeño del sistema de gestión y la información obtenida en cada una de las fases descritas.

7 Incumplimiento

Todas las partes, internas y externas, que tengan acceso a los sistemas de información en **SPMAS**, deben velar por el cumplimiento de la presente Política. En este sentido, las partes interesadas se responsabilizan de las consecuencias derivadas del incumplimiento de la presente Política de Seguridad de la Información, conforme a lo descrito en el II Convenio Colectivo Nacional de Servicios de Prevención Ajenos.

Nombre del representante de la Alta Dirección de SPMAS

RICARD SAYOS SUASI