POLÍTICA DE SEGURIDAD Y DE PROTECCIÓN DE DATOS PERSONALES

Documento de uso público

Contenido

Contenido

1. IDENTIFICACIÓN DE LA EMPRESA

Este documento expone la **Política Seguridad y Protección de Datos personales** (PSPD) de **MARVAX** como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de los requisitos del RGPD UE 2016/679 y el ENS (Esquema Nacional de Seguridad).

2. INTRODUCCIÓN

MARVAX depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad, o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos y Reglamento Europeo de Protección de Datos, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

MARVAX debe cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

MARVAX debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad y a la Ley Orgánica de Protección de Datos.

MARVAX aplicará los principios básicos de protección de datos y los demás requisitos del RGPD UE 2016/679 para el procesamiento de todos los datos personales a lo largo del ciclo de vida de la información mediante la adopción de los principios básicos de protección de datos de la presente política.

1.1. Prevención

MARVAX debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se implementarán las medidas mínimas de seguridad determinadas por el ENS, RGPD y la LOPD, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, **MARVAX** debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

1.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua, para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya preestablecido como normales.

1.3. Respuesta

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad de seguridad y de protección de datos personales.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos.
- Establecer protocolos de intercambio de información relacionada con incidentes con clientes y proveedores o encargados del tratamiento de protección de datos

1.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, **MARVAX** ha desarrollado planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

3. MISIÓN

MARVAX define la presente Política, de carácter obligatorio para empleados y empresas colaboradoras, teniendo como objetivo fundamental garantizar la seguridad de la información, la protección de datos personales y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes que puedan ocurrir.

Esta Política debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información y de los datos personales, de los que se sirve a **MARVAX** para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones:

- **Disponibilidad:** propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran.
- **Integridad:** propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada.
- **Confidencialidad:** propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados.
- **Autenticidad:** propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos.
- **Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Bajo estas premisas los objetivos específicos de la Seguridad de la información en **MARVAX** serán:

- Velar por la seguridad de la información y la protección de los datos personales, en las distintas dimensiones antes descritas.
- Gestionar formalmente la seguridad y la protección de los datos personales, sobre la base de procesos de análisis de riesgos.
- Elaborar, mantener y probar los planes de contingencias y continuidad de la actividad que se definan para los distintos servicios ofrecidos por la organización.
- Realizar una adecuada gestión de incidencias que afecten a la seguridad de la información y a la protección de los datos personales.
- Mantener informado a todo el personal acerca de los requerimientos de seguridad y de protección de los datos personales, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Cumplir con la reglamentación y normativa vigente.

Está Política:

- Se aprobará formalmente por la organización.
- Se revisará regularmente, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Se comunicará a todos los empleados y empresas externas qué trabajen con **MARVAX**.

4. ALCANCE

El alcance de esta política abarca todos los sistemas de información que respaldan las actividades realizadas por **MARVAX**, ubicadas en Calle Verbena de Valencia CP (46025) Valencia.

La presente es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de **MARVAX** para los servicios descritos.

5. DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

MARVAX considera la información y los datos personales como un activo estratégico y esencial para la continuidad de sus servicios.

La organización se compromete a:

- Proteger la información y los sistemas frente a pérdidas de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Cumplir con el Esquema Nacional de Seguridad, el RGPD, la LOPDGDD y toda la normativa aplicable.
- Aplicar medidas de seguridad proporcionadas a la criticidad y clasificación de los activos.
- Asignar a la Dirección la responsabilidad última en materia de seguridad, promoviendo la implicación de todo el personal en el cumplimiento de esta política.
- Realizar evaluaciones periódicas de riesgos y establecer planes de tratamiento cuando sea necesario.
- Fomentar la concienciación y formación en seguridad para empleados y colaboradores.
- Garantizar la gestión adecuada de incidentes y la mejora continua del sistema de seguridad.

6. MARCO NORMATIVO

Según la legislación vigente, las leyes aplicables a **MARVAX** en materia de Seguridad de la Información son:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 Abril del 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refun-dido de la Ley de Propiedad Intelectual.
- MARVAX cumple con la legislación citada y con todos sus requisitos.

MARVAX cumple con la legislación citada y con todos sus requisitos.

7. ORGANIZACIÓN DE LA SEGURIDAD

7.1 Comité: Funciones y Responsabilidades

Comité de Seguridad de la información

El **Comité de Seguridad de la Información** coordina la gestión de la seguridad en MARVAX y está formado por: Dirección, Responsable de Seguridad y Responsable del Sistema.

Funciones principales:

- Velar por el cumplimiento de esta Política y del ENS.
- Promover la mejora continua de la seguridad de la información.
- Coordinar esfuerzos en materia de seguridad y protección de datos.
- Aprobar normas, procedimientos y planes de mejora.
- Monitorizar riesgos, incidentes y auditorías de seguridad.
- Informar periódicamente a la Dirección del estado de la seguridad.

7.2 Roles: Funciones y Responsabilidades

Nivel de Gobierno – Dirección

- Asume la responsabilidad última en materia de seguridad.
- Establece requisitos, recursos y prioridades de seguridad.
- Aprueba la política, revisa auditorías y define el nivel de riesgo aceptable.
- Promueve la cultura de seguridad y la mejora continua.

Nivel de Supervisión – Responsable de Seguridad

- Supervisa el cumplimiento de la política y del ENS.
- Lidera el análisis y gestión de riesgos.
- Propone y coordina medidas de seguridad.
- Promueve formación, concienciación y auditorías.
- Apoya la gestión de incidentes y mantiene la documentación del SGSI.

Nivel Operativo – Responsable/Administrador del Sistema

- Aplica y mantiene las medidas de seguridad en los sistemas.
- Gestiona accesos, configuraciones y copias de respaldo.
- Supervisa el estado de seguridad técnico y reporta anomalías.
- Garantiza la trazabilidad y participa en la resolución de incidentes.

8. PROCEDIMIENTOS DE DESIGNACIÓN

El procedimiento de Designación se detalla a continuación.

La Dirección nombra al:

- Responsable de Seguridad, que reportará al Comité de Seguridad de la información y a la Dirección.
- Responsable del Sistema, que reportará al Responsable de Seguridad y al Comité de Seguridad de la información.

9. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DEL SISTEMA

El **Sistema de Gestión** está estructurado de forma que sea fácil de comprender y gestionar. La documentación se organiza de la siguiente manera:

Política de Seguridad y de protección de datos personales es un documento de alto nivel, La política está escrita a un nivel muy amplio, por lo que, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto.

Procedimientos Generales de Seguridad: Los Procedimientos generales afrontan tareas más genéricas en el marco Organizativo del Sistema de Gestión, indicando lo que hay que hacer, paso a paso. (Por ejemplo, Procedimiento general para auditorias, Procedimiento general para métricas e indicadores, etc)

Normas de Seguridad: Las Normas uniforman el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio

Procedimientos Operativos de Seguridad (POS): Los Procedimientos operativos afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

Instrucciones técnicas de Seguridad: determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.). Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar. Una instrucción técnica debe ser clara y sencilla de interpretar.

Registros y evidencias: Los registros, registran evidencias objetivas de la ejecución y terminación de actividades o trabajos realizados para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información alienados con los procedimientos, normas e instrucciones descritos en los apartados anteriores.

La gestión de nuestro sistema se encomienda al Responsable de Sistemas Informáticos y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos.

10. GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La organización gestionará los riesgos de seguridad de la información conforme a los principios del Esquema Nacional de Seguridad, aplicando un enfoque continuo y basado en riesgos.

El objetivo es **identificar, evaluar y tratar los riesgos** que afecten a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los sistemas que la soportan, manteniéndolos en niveles aceptables para la organización.

Para ello:

- Se aplicarán medidas técnicas y organizativas proporcionadas a la naturaleza de la información, los servicios prestados y la probabilidad e impacto de los riesgos.
- La gestión de riesgos será permanente y revisada regularmente, al menos una vez al año o cuando se produzcan cambios relevantes (nueva información tratada, modificación de servicios, incidentes graves o vulnerabilidades críticas).
- El proceso seguirá una metodología reconocida y documentada en informes formales de análisis y gestión de riesgos.
- La Dirección será responsable de aprobar los riesgos residuales y los planes de tratamiento del riesgo, garantizando la asignación de recursos necesarios.

11. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad y privacidad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la organización y difundida para que la conozcan todas las partes afectadas.

7.3 Principios de seguridad de la información

Esta Política de Seguridad y de Protección de Datos Personales complementa las políticas de seguridad de en diferentes materias:

- Gestión de Activos
- Uso aceptable de los sistemas de información.
- Seguridad de los equipos
- Autorización y control de accesos
- Adquisición, desarrollo y mantenimiento de los sistemas de información y de los datos personales.
- Mínimo privilegio
- Integridad y actualización del sistema
- Gestión del Cambio
- Protección de información almacenada y en tránsito
- Prevención ante otros sistemas de información interconectados

- Registro de actividad del usuario
- Seguridad en la gestión de comunicaciones y operaciones
- Protección de la información almacenada y en tránsito
- Eliminación y Destrucción de Información
- Navegación en Internet
- Uso Correo Electrónico
- Seguridad para la Gestión de Contraseñas
- Pantalla y Escritorio Limpio
- Protección frente a código malicioso y código móvil
- Gestión de la seguridad de la red
- Copias de Respaldo de la Información
- Gestión de la continuidad de los sistemas de información y de los datos personales
- Resiliencia de los sistemas de información y de los datos personales
- Gestión de incidentes de seguridad y de los datos personales
- Cumplimiento
- Profesionalidad
- Acciones Correctivas
- Mejora continua del proceso de seguridad

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. 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.

7.4 Protección de Datos y Privacidad

La Ley Orgánica de Protección de Datos (LOPD) y el RGPD, tratan de garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, y resulta de aplicación a los datos de carácter personal registrados tanto informáticamente como en soporte papel.

12. OBLIGACIONES DEL PERSONAL

Todos los miembros de **MARVAX** tienen la obligación de conocer y cumplir esta Política, siendo responsabilidad del Comité de Seguridad y privacidad disponer los medios necesarios para que la información llegue a los afectados.

La presente Política debe ser conocida por todos los usuarios externos y por las empresas que accedan, gestionen o traten información o datos personales de **MARVAX**.

El conjunto de Políticas, normas y procedimientos complementarios a esta Política también deberán ser adecuadamente comunicados y puestos en conocimiento de las personas, empresas e instituciones afectadas o implicadas en cada caso. TERCERAS PARTES

Cuando **MARVAX** preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, 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 **MARVAX** utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante

13. RESOLUCIÓN DE CONFLICTOS Y CONFLICTOS DE LEGISLACIÓN

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de protección de datos y seguridad de la información corresponderá, en última instancia, a la Dirección, asistida por el Comité de Seguridad de la Información y, cuando proceda, por el delegado de protección de datos, la resolución de conflictos.

Esta política está destinada a cumplir con las leyes y reglamentos en el lugar de establecimiento y de los países en los que opera **MARVAX**. En caso de conflicto entre esta política y las leyes y reglamentos aplicables, prevalecerá esta última.

14. DESARROLLO NORMATIVO Y REVISIÓN DE LA PRESENTE POLÍTICA

Corresponderá a la Dirección de **MARVAX**, a propuesta de los miembros que integran la estructura organizativa de la presente política y asistida por el Comité de Seguridad de la Información y, cuando proceda, por el delegado de protección de datos, la adopción de los procedimientos, guías e instrucciones técnicas necesarios para el desarrollo de la presente Política.

En el proceso de desarrollo normativo podrá requerirse la colaboración de las unidades organizativas que componen la estructura orgánica de la **MARVAX**.

La presente política se someterá a un proceso de revisión, al menos anual, a fin de adaptarse a las circunstancias técnicas u organizativas y evitar su obsolescencia.

15. LISTA DE CONTROL DE CAMBIOS

Versión	Fecha de entrada en vigor	Descripción del cambio
01	06/10/2025	Creación del documento