Política de Gestión de Servicios de Ciberseguridad

01 de septiembre de 2023

VASS

complex made simple

(**)
VASS Madrid
CMMI-DEV v2.0 (Staged): Maturity Level, Web Portal Development Projects
UNE-EN ISO 9001:2015 Diseño, desarrollo e implantación portales web y plataformas de soporte a los procesos de negocio y a la gestión documental.
UNE-EN ISO 14001:2015 Diseño, desarrollo e implantación portales web y plataformas de soporte a los procesos de negocio y a la gestión documental.

Índice

1. Aprobación y entrada en vigor

El cumplimiento de esta Política de Gestión de Servicios de Ciberseguridad es obligatorio a partir del 1 de septiembre de 2023, de forma indefinida, para todo el personal dentro del alcance.

Esta versión de la Política de Gestión de Ciberseguridad es efectiva desde el 1 de septiembre de 2023 y hasta que sea reemplazada por una nueva versión.

2. Objeto

La Dirección de VASS Consultoría de Sistemas SL (en adelante VASS), dentro de la estrategia definida para el desarrollo del negocio, considera la adecuada gestión de los servicios de Ciberseguridad, como un servicio fundamental dentro del catálogo de servicios de la empresa. Por ello, se compromete a velar por la adecuada gestión de los servicios de ciberseguridad prestados por la organización, además de garantizar la seguridad de la información, la gestión de la privacidad y la continuidad de este negocio, con objeto de ofrecer a todos sus grupos de interés las mayores garantías en cuanto a la calidad de dichos servicios.

La dirección de VASS se compromete a gestionar y proteger su información y sus servicios en los proyectos dentro del ámbito de la ciberseguridad, de forma adecuada mediante la implantación, mantenimiento y mejora de un **Sistema de Gestión del Servicio de Ciberseguridad** (en adelante, **SGS**) aplicando los requisitos de la Norma UNE-ISO/IEC 20000-1 y de sus partes interesadas, para garantizar que los servicios TI contemplados en el alcance ofrecen los niveles de calidad requeridos por sus destinatarios y se gestionan de acuerdo con las exigencias contempladas en dicha norma,

Asimismo, la Dirección General de VASS Consultoría de Sistemas se compromete a implantar, mantener y mejorar un **Sistema de Gestión de la Seguridad de la Información** (en adelante **SGSI**), un **Sistema de Gestión de la Privacidad** (en adelante **SGP**) y otro de la **Gestión de la Seguridad de la Información en los Servicios en la nube**, todos ellos integrados, aplicando los requisitos de las Normas UNE-ISO/IEC 27001, UNE-EN ISO/IEC 27701 y UNE-EN ISO/IEC 27018 y de sus partes interesadas para garantizar que los servicios contemplados en el alcance ofrecen los niveles de seguridad de la información y privacidad requeridos por sus destinatarios y se gestionan de acuerdo con las exigencias contempladas en dichas normas. El **SGSI** será definido, implementado y mejorado según las directrices establecidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, aplicándose en su nivel Alto, para los Servicios de Ciberseguridad.

Finalmente, la dirección de VASS se compromete a implantar, mantener y mejorar un **Sistema de Gestión de la Continuidad del Negocio** (en adelante **SGCN**), aplicando los requisitos de la Norma UNE-EN ISO 22301 y de sus partes interesadas, para garantizar la continuidad de los servicios TI contemplados en el alcance y que ello se gestiona de acuerdo con las exigencias contempladas en dicha norma.

El presente documento constituye la política de Gestión de Servicios de Ciberseguridad de VASS que establece las directrices y principios que regirán el modo en que VASS gestionará sus servicios a través de los Sistemas de Gestión definidos.

3. Términos y Definiciones

Servicio de TI. Solución informática completa que cubre unas necesidades específicas para el negocio de la organización y que se entrega y mantiene de manera que se libere a los usuarios de las complejidades internas inherentes de la tecnología.

Parte interesada: Persona o grupo que tiene un interés en el desempeño o éxito de la organización.

Activo: En relación con la gestión de servicios, se refiere a cualquier información o elemento relacionado que tenga valor para la organización.

Elemento de Configuración: Elemento que es necesario controlar para proveer uno o varios servicios.

Incidencia: Interrupción inesperada de un servicio, una reducción en la calidad de un servicio o un evento que todavía no ha tenido impacto en el servicio para el cliente o para el usuario.

Problema: Causa de una o más incidencias reales o potenciales

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de medidas.

4. Alcance

El alcance de esta política comprende los servicios TI que presta VASS en el ámbito de la ciberseguridad, así como los sistemas y tecnologías de la información que soportan los mecanismos de seguridad de la información, gestión de la privacidad y continuidad de los procesos de negocio y los activos de información empleados en el desarrollo, gestión y prestación, mantenimiento, mejora y continuidad de proyectos de ciberseguridad (ANTIDDOS, Proyectos de mensajería administrado por VASS, Proyectos de mensajería sin administración de VASS, Soporte y gestión de dispositivos (SOC), virtual data center (VDC), SASE - Security Edge, Tráfico limpio de correo avanzado, UTM gestionado, WAF gestionado, Cyberthreats (Digital Risk Protection), Gestión de vulnerabilidades (Vulnerability scanning), SIEM Management, Redes limpias) y que se prestan por los departamentos o áreas de VASS, tanto al personal interno, como a clientes externos.

5. Objetivos de la Política de Gestión de Servicios de TI

VASS es una empresa española de capital 100% privado, proveedora de soluciones digitales cuya misión es ayudar a los clientes a transformar las oportunidades en negocio.

Para el cumplimiento de su Misión, la prestación de los Servicios y el cumplimiento de sus objetivos, VASS depende de sistemas TIC. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para garantizar que los servicios contemplados en el alcance ofrecen los niveles de calidad requeridos por sus destinatarios y que se garantiza la seguridad de la información, incluida la gestionada a través de servicios en la nube, la privacidad de los datos personales y la continuidad del negocio.

Dentro de este contexto, los objetivos de la presente Política del Sistema de Gestión del servicio:

- Asegurar que los servicios de ciberseguridad están alineados con las necesidades de sus clientes y usuarios.
- Mejorar la comunicación entre el personal que participa en la prestación de los servicios de ciberseguridad y los clientes y usuarios de dichos servicios.
- Incrementar la eficacia y eficiencia de los procesos internos de prestación de los servicios de ciberseguridad.
- Ofrecer a los clientes y usuarios servicios de mayor calidad.
- Reducir los riesgos asociados a los servicios de ciberseguridad, incluyendo los asociados a la seguridad de la información, protección de datos personales y continuidad del negocio.
- Nombrar responsables de los Sistemas de Gestión, encargado de gestionar los sistemas y velar por el desarrollo, mantenimiento y mejora de los mismos.
- Nombrar un Responsable del Servicio, un Responsable de Seguridad y un Responsable de Información y asegurar que disponen de los recursos necesarios para llevar a cabo las tareas necesarias.
- Establecer una metodología de revisión, auditoría y mejora continua de los Sistemas de Gestión, siguiendo un ciclo PDCA que garantice el mantenimiento continuo de los niveles gestión deseados.
- Gestionar la prestación y continuidad de los servicios realizados a los clientes de forma eficaz y eficiente, dentro de un ciclo de vida que permita la mejora continua de los procesos implantados y de los Sistemas de Gestión en general.
- Establecer periódicamente un conjunto de objetivos e indicadores en materia de gestión, que permitan a la dirección llevar a cabo un adecuado seguimiento del nivel de gestión y cumplimiento de los objetivos.
- Garantizar que el personal de la organización dentro del alcance dispone del suficiente conocimiento sobre las políticas de gestión de los servicios y sus funciones y obligaciones en el ámbito de los Sistemas de Gestión y son responsables de cumplirlas.
- Garantizar que las personas de la organización son formados y concienciados en materia de seguridad de la información, protección de datos y continuidad de negocio.
- Asegurar que los incidentes son correctamente identificados, gestionados y resueltos.
- Cumplir con todos los requisitos legales, normativos, reglamentarios aplicables y obligaciones contractuales.
- Asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- Asegurar la continuidad de los procesos de negocio incluidos dentro del alcance.
- Asegurar la protección de los datos personales, cumpliendo la normativa vigente en este ámbito.

6. Organización de la Gestión de Servicios de Ciberseguridad

6.1 Comités: Funciones y Responsabilidades

La Dirección de VASS se compromete a destinar los recursos y medios necesarios para establecer, implantar, mantener y mejorar el SGS, manteniendo un adecuado balance entre coste y beneficio, así como a demostrar liderazgo y compromiso respecto a este.

Con objeto de garantizar el cumplimiento de los intereses de la Dirección y asegurar una correcta gestión de los servicios se constituye el **Comité de Gestión IT** que responde a la Dirección General y está coordinado por un miembro del Comité de Dirección.

Las competencias del Comité de Gestión IT y los miembros que forman parte de él se encuentran detallados en la documentación de los Sistemas de Gestión.

6.2 Roles: Funciones y Responsabilidades

Los diferentes roles serán nombrados por el Comité de Dirección y se tendrán en consideración los criterios de representación indicados, la idoneidad del personal a designar, así como la predisposición de los candidatos para ejercer las funciones que les correspondan. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Los roles establecidos en la organización se describen en la documentación de los Sistemas de Gestión, y son básicamente las que a continuación se indican:

- **Responsable de Información:**
  - El responsable de información se encarga de que el sistema de información funcione sin contratiempos y eficientemente.
  - El responsable de la Información deberá coordinar con el Responsable de Sistemas la mejora de los sistemas informáticos. Asimismo, organizan la formación del personal, gestionan presupuestos. Organiza el mantenimiento de los sistemas informáticos y pone en práctica sistemas de respaldo en caso de que surja un fallo de TIC.
- **Responsable de seguridad**
  - Establecer políticas relacionadas con la seguridad, unificando criterios y procesos.
  - Garantizar el cumplimiento de los requisitos de seguridad de la información del ENS y cumplimiento con las leyes vigentes en el área de la información digital y física, tanto por parte de terceros con quienes guarde relación como por parte de sus colaboradores.
  - Elaborar la estrategia de respuestas ante incidentes que pongan en riesgo la seguridad de la información. Esto debe hacerlo con la ayuda de un equipo técnico y de otras personas que en una situación de este tipo puedan asumir funciones complementarias.
  - Supervisar el acceso a las cuentas y perfiles en las que pueda haber información confidencial, así como elaborar planes de restauración de información y de continuidad del negocio.
  - Liderar las investigaciones forenses, tanto digitales como en soportes tradicionales, para revelar las causas de irregularidades ligadas a la gestión de la información.

    - Comunicar las brechas de seguridad a la AEPD y las infecciones por malware al INCIBE y/o al CCN.
- **Responsable de Sistemas**
    - Se encarga de establecer conexiones entre los sistemas de información.
    - Debe además establecer propuestas de mejora y coordinar al equipo
    - técnico. Controlar el proceso del flujo de datos y la dotación tecnológica que
    - necesita la sede electrónica.
    - Por otro lado, debe supervisar los cambios y estar al tanto de las nuevas
    - necesidades tecnológicas y de los requisitos de la seguridad de la
    - información adaptándose y adelantándose a las nuevas necesidades de la
    - sede electrónica y a los requisitos de los cambios impuestos por la evolución
    - tecnológica.
- **Responsable del Servicio**
    - Realizar las funciones de administración del servicio.
    - Gestionar las incidencias con los trámites del servicio.
    - Gestión de accesos de usuarios.
    - Controlar el buen funcionamiento del servicio.
    - Resolución de dudas o incidencias del servicio.
    - Contacto con los proveedores de la plataforma para la resolución de incidencias detectadas.

7. Sistemas de Gestión

7.1 Objetivos de los Sistemas de Gestión y su Planificación

Los objetivos de los Sistemas de Gestión se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance de los Sistemas de Gestión.
- Requisitos de negocio y de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar un adecuado nivel y calidad del servicio.
- Factores internos y externos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad y afecta a su desempeño en la gestión de los servicios.

Asimismo, la planificación para la consecución de los objetivos establecidos se realizará considerando las acciones a realizar y su responsable, los recursos y plazos necesarios y los indicadores para evaluar el resultado/cumplimiento.

7.2 Establecimiento, despliegue y mejora de los Sistemas de Gestión

El establecimiento y despliegue de los Sistemas de Gestión de VASS se iniciará a partir del Análisis de Riesgos con el fin de asegurar que de los Sistemas de Gestión puedan lograr sus resultados previstos, prevenir o reducir efectos no deseados y lograr la mejora continua de los Sistemas y de los servicios, que permitirá determinar el nivel de riesgo e identificar las acciones necesarias para el tratamiento del riesgo y llevarlo a un nivel aceptable, así como las oportunidades de mejora, considerando las cuestiones internas y externas y los requisitos de las partes interesadas.

Las acciones deberán implantarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada, mediante procedimientos, normativas, instrucciones técnicas, y cualquier otra documentación que así se considere, revisados y aprobados por el Comité de Gestión IT.

Se realizarán auditorías que revisen y verifiquen el cumplimiento de los Sistemas de Gestión con los requisitos de las Normas de referencia, por lo que, en caso necesario, el personal afectado por el alcance deberá colaborar en estas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo.

8. Política de Gestión de Servicios de TI

El compromiso adquirido por la Dirección de VASS para implantar, mantener y mejorar un SGS se traduce en el siguiente conjunto de políticas:

- Todo el personal que interviene en la prestación de servicios TI dentro del ámbito de los proyectos de ciberseguridad, debe medir, revisar y asegurar la mejora continua de las características de los servicios TI prestados a los usuarios.
- Se debe asegurar que las características de los servicios TI prestados son apropiados para los propósitos del proveedor del servicio.
- Todos los servicios TI proporcionados deberán estar adecuadamente monitorizados con el objeto de que la organización sea capaz de proporcionar a los clientes de los servicios toda la información necesaria para realizar el seguimiento de las características más relevantes de los mismos.
- La organización mantendrá su compromiso de satisfacer todos los requisitos del servicio.
- El personal del servicio colaborará en la correcta identificación de los requerimientos de disponibilidad y de continuidad de los servicios TI proporcionados por la organización.
- Se desarrollarán planes de continuidad de los sistemas como parte de su plan general de continuidad de negocio y actividades de recuperación.
- Todos los servicios TI prestados por la organización estarán adecuadamente presupuestados, considerando tanto los costes directos como los indirectos, e incluyendo en dichos presupuestos los costes iniciales y los derivados del mantenimiento periódico de los activos asociados a cada servicio.
- La organización deberá realizar una monitorización periódica del presupuesto y de los costes directos e indirectos del servicio.
- Todo el personal implicado en la prestación de servicios TI se deberá asegurar de que los servicios ofrecidos satisfagan las demandas de servicio de sus respectivos usuarios.
- La organización dispondrá de un gran compromiso de mejora continua del Sistema de Gestión y de los servicios que se prestan a los clientes.
- Se identificarán los requisitos de seguridad de la información de los servicios prestados por la organización.
- Se analizarán los riesgos de seguridad de la información de todos los servicios TI prestados por la organización, y se establecerán los controles asociados necesarios para mitigar los riesgos identificados.
- Se identificarán los requisitos de capacidad tanto actual como futura, para asegurar que se pueden prestar los servicios, cumpliendo con las expectativas del cliente y con los acuerdos de nivel del servicio acordados.
- Se celebrarán reuniones periódicas con los clientes de los servicios TI prestados por la organización, para identificar sus necesidades, efectuar un seguimiento del nivel de satisfacción de los servicios prestados, e identificar cualquier cambio o petición de mejora sobre los servicios.

- Se establecerán acuerdos de nivel de servicio con los suministradores involucrados en la prestación del servicio TI, a fin de asegurar que los niveles de servicio acordados cumplen con los niveles de servicio que la organización ha suscrito con sus clientes.
- Se establecerán mecanismos de detección, análisis y reporte para que se puedan informar a los responsables tanto regularmente como cuando se produzcan anomalías en los niveles de prestación de los servicios y actuar en consecuencia ante una desviación significativa de los parámetros que se hayan preestablecido como normales.
- Todo el personal implicado en los servicios participará en la resolución de los incidentes que se identifiquen, con el objetivo de minimizar el impacto y asegurar la continuidad y disponibilidad del servicio prestado dentro de los valores de nivel de servicio acordados con el cliente.
- Todos los problemas identificados, tanto a raíz de las actividades de identificación preventiva, como los escalados a partir de un incidente, serán adecuadamente analizados hasta identificar la causa subyacente de error, y se establecerán las acciones correctivas necesarias para subsanar o paliar sus efectos y para solventar el problema raíz.
- Todo el personal involucrado en la gestión de servicios TI registrará, mantendrá y llevará a cabo un adecuado seguimiento de los elementos de configuración a su cargo y sus características.
- Todos los cambios que se produzcan sobre cualquier aspecto de los servicios TI, provistos por la organización, deberán haber sido iniciados por una propuesta de cambio formal y autorizados de acuerdo al procedimiento de gestión de cambios.
- Todas las peticiones de cambio deberán ser analizadas antes de su aprobación para ver su impacto en el servicio y su impacto sobre los requisitos de seguridad de la información.
- Se deberá controlar el pase a producción de los elementos de configuración según los procedimientos definidos de gestión de entrega y despliegue.
- Se establecerá un Plan de Formación y Concienciación en materia de Gestión de los Servicios TI, que ayude a todo el personal implicado a conocer y cumplir las actividades de gestión definidas.

9. Terceras Partes

En el caso de que el proceso esté operado por terceros:

- Se deberán proporcionar evidencias de cumplimiento de todos los requisitos (en el caso de que el proveedor del servicio opere todos o parte de los procesos directamente) o evidencias del cumplimiento de los requisitos, donde deberán existir evidencias del gobierno de los procesos, o parte de los procesos (en el caso de servicios operados por terceros y que el proveedor de servicio no opera directamente).
- El proveedor de servicio deberá:
  - Demostrar responsabilidad sobre los procesos y autoridad para exigir adhesión a los mismos.
  - Controlar la definición de los procesos e interfaces con otros procesos.
  - Determinar el comportamiento de los procesos y la conformidad con los requisitos de los procesos.
  - Controlar la planificación priorizando las mejoras de los procesos.

10. Desarrollo de la Política

Esta Política de Gestión de Servicios de Ciberseguridad complementa las políticas de VASS en materia de Calidad, Seguridad de la Información y Medio Ambiente.

La Política de Gestión de Servicios de Ciberseguridad se desarrollará por medio de unos procedimientos que afronten aspectos específicos de la gestión de dichos servicios. Los

procedimientos estarán 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.

La Política se desarrollará aplicando los siguientes principios mínimos:

- Organización e implantación del proceso de gestión de los servicios.
- Alineación de los servicios con los objetivos de negocio.
- Planificación e implantación de nuevos servicios o servicios cambiados.
- Gestión de los niveles de servicios.
- Relaciones con el negocio y suministradores.
- Seguridad de la Información.
- Análisis y gestión de los riesgos.
- Gestión de personal y la capacidad de los servicios.
- Gestión de la continuidad y disponibilidad de los servicios,
- Resolución de incidentes y problemas.
- Integridad y actualización del sistema.
- Registro de actividad.
- Mejora continua de la gestión de servicios.

Las normativas de seguridad estarán disponibles en la Intranet de VASS.

11. Publicación

La presente Política del Sistema de Gestión del Servicio de Ciberseguridad, aprobada por el Comité de TI, es conocida y suscrita por todo el personal de VASS que se encuentre dentro del alcance de los Sistemas de Gestión, conforme a las exigencias de la Dirección, y por el personal de los proveedores del servicio dentro del alcance. Tras cada revisión, la política será nuevamente publicada y comunicada al personal dentro del alcance.

La política para el alcance definido estará disponible en la Intranet de VASS.

12. Revisión

Esta Política del Sistema de Gestión del Servicio de Ciberseguridad será revisada, como mínimo, anualmente, o cada vez que se produzcan cambios importantes organizativos o en la infraestructura. Cualquier cambio sobre en las políticas deberá ser aprobado por el Comité de Gestión IT.