POLÍTICA

SEGURIDAD DE LA INFORMACIÓN

POL.01

versión 1.0

18.02.2025

INFORMACIÓN PÚBLICA

CONTROL DE VERSIONES

VERSIÓN	FECHA:	MODIFICACIÓN
1.0	18.02.2025	Versión inicial del documento

RUTA DE APROBACIÓN

VERSIÓN	REALIZADO POR:	REVISADO POR:	APROBADO POR:
1.0	Responsable de Seguridad	Dirección	Dirección
	Fecha: **18.02.2025**	Fecha: **18.02.2025**	Fecha**18.02.2025**

RESPONSABILIDAD

DISTRIBUCIÓN	ARCHIVO	ACTUALIZACIÓN
Dirección	Responsable del SGSI	Comité de Seguridad

INDICE DE CONTENIDOS

1. CONTEXTO

La información constituye para la práctica totalidad de los procesos de negocio de **VASALTO TECH AND TALENT, S.A** (en adelante, **VASALTO**), el hilo conductor imprescindible para la ejecución de los mismos con garantías de eficiencia y calidad, alcanzando, con ello, el cumplimiento de los objetivos estratégicos formalmente establecidos por la **Dirección**.

Las dimensiones principales de la seguridad de la información que deben ser garantizadas en la ejecución de cualquier proceso de negocio son:

- **Confidencialidad:** Garantiza que la información solo se encuentre accesible a personas, entidades o procesos autorizados.
- **Integridad:** Garantiza que la información es generada, modificada y eliminada solo por personas, entidades o procesos autorizados.
- **Disponibilidad:** Garantiza que la información se encuentre accesible cuando las personas, entidades o procesos autorizados lo precisen.
- **Trazabilidad:** Garantiza que la información relativa a los accesos y actividad ejecutada por personas, entidades o procesos se encuentra disponible para cualquier análisis de patrones de comportamiento anómalos que deba ser efectuado.

Por otro lado, se presentan otras dimensiones de la seguridad, tales como la **autenticación de las partes** o el **no repudio** que, de igual forma, deben ser garantizadas cuando el valor de seguridad de la información en el contexto del proceso de negocio en el que esté siendo almacenada, procesada, o transmitida, así lo precise.

La **Política de Seguridad de la Información** se basa en la adopción de principios claros y bien definidos que aseguren el cumplimiento de las directrices estratégicas, los requerimientos legales, así como los de carácter contractual formalizados con terceros o *stakeholders* y, por tanto, se constituye como el instrumento principal en el que se apoya **VASALTO** para la utilización segura de las tecnologías de la información y comunicaciones.

La normativa (estándares, procedimientos e instrucciones de seguridad) que emane o se deriven de la **Política de Seguridad de la Información** de **VASALTO** pasará a formar parte de la misma una vez haya sido divulgada, siendo de obligado cumplimiento para la totalidad de los empleados y terceras partes que hagan uso de la información propiedad de **VASALTO**.

La **Dirección** de **VASALTO** asegurará que esta **Política de Seguridad de la Información** es entendida e implantada en toda la organización, facilitando los recursos necesarios para la consecución de los objetivos definidos en este marco de actuación.

2. OBJETIVOS

La **Política de Seguridad de la Información** queda establecida como el documento de alto nivel que formaliza las distintas directrices de actuación en materia de seguridad adoptadas por **VASALTO**, y que serán desarrolladas en mayor detalle en la correspondiente normativa de seguridad elaborada a tales efectos.

Bajo esta premisa, por tanto, la **Política de Seguridad de la Información** contempla los siguientes objetivos principales:

- Dar cumplimiento a la normativa legal de aplicación en el ámbito de la seguridad de la información.

- Contribuir a cumplir con la misión y objetivos estratégicos formalizados por **VASALTO**.
- Alinear la seguridad de la información como activo principal con los requerimientos demandados por el negocio mediante la formalización del **modelo de valor de la información** y la ejecución del proceso de análisis y evaluación de los riesgos a los que se encuentran expuestos los distintos activos de información, alcanzando la definición de una estrategia para la mitigación de los riesgos relacionados con el entorno de la seguridad de la información.
- Garantizar la protección adecuada de los distintos activos de información en función del grado de sensibilidad y criticidad alcanzado por los mismos (valor de seguridad de los activos de información según las distintas dimensiones consideradas con la aplicación del criterio de herencia y el principio de proporcionalidad).
- Garantizar una capacidad de respuesta eficaz a eventuales incidentes de seguridad de la información, minimizando el respectivo impacto operacional, financiero y reputacional.
- Facilitar el dimensionamiento de los recursos necesarios para la correcta implantación de las medidas de seguridad de índole técnica y organizativa recogidas en la normativa de seguridad documentada a tales efectos.
- Fomentar el uso de buenas prácticas en materia de seguridad de la información, así como crear la cultura de seguridad pertinente en el contexto de la estructura organizativa de **VASALTO**.
- Establecer los mecanismos de revisión, monitorización, auditoría y mejora continua con el objeto de mantener los niveles de seguridad oportunos demandados por el modelo de negocio de **VASALTO**.

3. ALCANCE

La **Política de Seguridad de la Información** contempla en su alcance la totalidad de los activos de información existentes en **VASALTO** y que actúan como infraestructura de soporte para la posible ejecución de los procesos de negocio y la prestación de servicios.

4. MARCO NORMATIVO

La formalización de la **Política de Seguridad de la Información**, así como la normativa de seguridad que se derive de la misma, tendrá en consideración e integrará la siguiente normativa legal aplicable:

- **Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante, RGPD – Reglamento General de Protección de Datos)**, 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.
- **Ley Orgánica, 3/2018, de 5 de diciembre de 2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, Ley 3/2018).**
- **Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (en adelante, LSSICE).**
- **Ley 6/2020, de 11 de noviembre,** reguladora de determinados aspectos de los servicios electrónicos de confianza que adapta el ordenamiento jurídico español al Reglamento (UE) 910/2014 (también conocido como EIDAS)**.**
- **Texto refundido de la Ley de Propiedad Intelectual,** aprobado mediante el Real Decreto Legislativo 1/1996, de 12 de abril de 1996. Esta normativa ha sido modificada por varias leyes, incluyendo la Ley 21/2014, que traspone el contenido de las directivas europeas a la legislación española, y la Ley 2/2019 que incorpora la Directiva 2014/26/UE y la Directiva (UE) 2017/1564**.**

5. PRINCIPIOS

Con el objeto de garantizar el cumplimiento de los objetivos de seguridad identificados con anterioridad, la **Política de Seguridad de la Información** formaliza la aplicación de determinados principios de seguridad.

5.1. SEGURIDAD COMO PROCESO INTEGRAL

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con los sistemas de información utilizados como soporte para la ejecución de los procesos de negocio. En este sentido, por tanto, todas las actividades de seguridad serán ejecutadas bajo esta perspectiva, evitando cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en la ejecución de los procesos de negocio, y la de los responsables jerárquicos con el objeto de evitar que el desconocimiento, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad de la información.

5.2. GESTIÓN DE LA SEGURIDAD BASADA EN LOS RIESGOS

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno de información controlado, minimizando los riesgos hasta niveles aceptables formalizados por la **Dirección**.

La reducción del riesgo hasta tales niveles se alcanzará mediante la aplicación de medidas de seguridad, de forma equilibrada y proporcionada a la naturaleza de la información tratada, los servicios a prestar y los riesgos a los que estén expuestos los distintos activos de información utilizados.

5.3. PREVENCIÓN, DETECCIÓN Y RESPUESTA

La seguridad de la información debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar las vulnerabilidades existentes, y lograr que las amenazas no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información o los servicios prestados.

Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección estarán orientadas a la alerta temprana de cualquier escenario de materialización de amenazas.

Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5.4. EXISTENCIA DE LÍNEAS DE DEFENSA

Se deberá garantizar que la estrategia de protección queda conformada por múltiples capas de seguridad, dispuestas de forma que, cuando una de las capas se vea comprometida, se pueda reaccionar adecuadamente frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que puedan propagarse.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

5.5. VIGILANCIA CONTINUA Y REEVALUACIÓN PERIÓDICA

La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de seguridad de los activos de información permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

6. TERCERAS PARTES

Cuando **VASALTO** requiera de la participación de terceras partes para la prestación de un servicio, les hará participes de la normativa de seguridad que sea de consideración en el contexto de dicha colaboración, quedando éstos sujetos a las obligaciones establecidas en dicha normativa.

Cuando algún aspecto de la normativa de seguridad no pueda ser satisfecho por una tercera parte, se requerirá la autorización del **Responsable de Seguridad** previa identificación de los riesgos en que se incurre y la forma de tratarlos, no siendo posible la formalización de la contratación con carácter previo a la obtención de dicha autorización. En cualquier caso, estas autorizaciones, en función de su categorización serán reportadas al **Comité de Seguridad de la Información** con el objeto de que se adopten las decisiones oportunas.

7. REVISIÓN

La **Política de Seguridad de la Información** será revisada anualmente por el **Comité de Seguridad de la Información** o cuando exista un cambio significativo (enfoque de la gestión de la seguridad, circunstancias del negocio, cambios legales, cambios en el ambiente técnico, recomendaciones realizadas por autoridades de control y tendencias relacionadas con amenazas y vulnerabilidades) que obligue a ello.

En el caso de que se obtenga una nueva versión de la **Política de Seguridad de la Información**, será precisa la aprobación formal de **Dirección** con carácter previo a su divulgación.

8. ENTRADA EN VIGOR

Texto aprobado por la **Dirección** el día **18 de febrero de 2025**.

Su entrada en vigor supone la derogación de cualquier otra política que existiera a tales efectos.

La Dirección