

**POLÍTICA DE SEGURIDAD DE LA
INFORMACIÓN DE**



BEWOR TECH S.L.

B19603968

PARQUE EMPRESARIAL CORTIJO DEL CONDE.

C/ Pago de Cambea, 14, Nave 7, 18015 Granada - España

ÍNDICE

| | |
|--|----------|
| INFORMACIÓN GENERAL | 3 |
| CONTROL DOCUMENTAL | 3 |
| ESTADO FORMAL | 3 |
| CONTROL DE VERSIONES | 3 |
| | |
| POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN | 4 |
| 1. INTRODUCCIÓN | 4 |
| 2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN | 5 |
| 3. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN | 6 |
| 4. ADMINISTRACIÓN DE LA POLÍTICA DE SEGURIDAD | 7 |
| 5. ALCANCE Y ÁMBITO DE APLICACIÓN | 7 |
| 6. COMUNICACIÓN | 8 |
| 7. POLITICA DE PROTECCION DE DATOS PERSONALES | 8 |

INFORMACIÓN GENERAL

CONTROL DOCUMENTAL

| |
|---|
| Clasificación de seguridad: Público |
| Versión: 2.0 |
| Fecha edición: 17/11/2022 |
| Fichero: POL-1-Política_Seguridad_Información |
| Código: POL-1 |
| Estado formal |
| Preparado por: Néstor Castillo Morales, Fecha: 17/11/2022 |
| Revisado por: Patricia Bodelón Álvarez, Fecha: 21/11/2022 |
| Aprobado por: Vicente Jesús Serrano Pérez, Fecha: 19/12/2022 |

CONTROL DE VERSIONES

| Versión | Partes que cambian | Descripción cambio | Autor Cambio | Fecha de Cambio |
|---------|--------------------|--------------------|-----------------|-----------------|
| 1.0 | Original | Creación documento | Néstor Castillo | 02/10/2021 |
| 2.0 | Original | Revisión documento | Néstor Castillo | 17/11/2022 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

1. INTRODUCCIÓN

Este documento contiene la Política de Seguridad de la Información (en lo sucesivo PSI) de BEWOR TECH S.L., de acuerdo al Sistema de Gestión de la Seguridad de la Información (en adelante SGSI), la cual implementa en sus actividades relacionadas a la prestación de servicios de certificación y microservicios.

Este documento es el resultado del compendio de documentos relativos a los procesos que garantizan la seguridad de la información de los procesos del Prestador de Servicios de Confianza y de Microservicios.

2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Dirección de BEWOR TECH S.L. reconoce la importancia de identificar y proteger sus activos de información, y en especial los de los clientes, evitando la pérdida, la divulgación, modificación y utilización no autorizada de toda su información, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

Es responsabilidad de la Dirección de BEWOR TECH S.L.:

1. Establecer periódicamente objetivos sobre la gestión de la Seguridad de la Información, y las acciones necesarias para su desarrollo.
2. Establecer la sistemática de análisis del riesgo, evaluando el impacto y las amenazas.
3. Implementar las acciones necesarias para reducir los riesgos identificados que se consideren inaceptables, según los criterios establecidos por el Comité de Seguridad.
4. Aplicar los controles necesarios y sus correspondientes métodos de seguimiento.

5. Cumplir con los requisitos asumidos por BEWOR TECH S.L., legales, reglamentarios, de cliente y las obligaciones contractuales de seguridad.

6. Promover la concientización y formación en materia de seguridad de la información a todo el personal de BEWOR TECH S.L.

7. Aportar los recursos necesarios para garantizar la continuidad del negocio de la empresa.

La Seguridad de la Información se caracteriza como la preservación de:

a) su disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

b) su confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información;

c) su integridad, asegurando que la información se mantiene invariable y trazable.

La dirección de BEWOR TECH S.L. nombra al Responsable de Seguridad de la Información como responsable directo en el mantenimiento de la política de seguridad de la información, por brindar consejo y guía para su implementación.

3. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

Los objetivos de seguridad de la información se definen por parte del Comité de seguridad de la información en las reuniones periódicas, en base a la documentación y registros aportados por el SGSI, los cuales serán aprobados por el Comité estratégico o en su defecto por la Dirección.

Las metas y objetivos estarán de acuerdo con la Política de BEWOR TECH S.L. y el análisis del contexto.

Los objetivos de seguridad se agrupan entorno a los siguientes bloques de trabajo:

- Protección del conocimiento, la información y los datos.
- Protección de las tecnologías de la información y las comunicaciones.
- Protección de las instalaciones, edificios y estancias.
- Protección de los activos de la compañía.
- Protección de la continuidad del negocio.
- Cumplimiento con los estándares legales y normativos.

Esta documentación (que incluye no-conformidades, acciones correctoras y preventivas, auditorías internas, registros de formación, etc.) tiene que servir como base de referencia para el establecimiento de objetivos medibles y cuantificables orientados a la mejora continua del servicio.

Los objetivos quedan recogidos en el documento de seguridad que da soporte y apoyo al sistema de gestión de seguridad de la información.

Todo tratamiento de datos personales deberá respetar los requisitos normativos exigibles y aplicables al nivel de riesgo que implique para la persona física cuyos datos personales se tratan. Se deberá tener en cuenta para su aplicación, los recursos necesarios y el equipo de trabajo involucrado.

4. ADMINISTRACIÓN DE LA POLÍTICA DE SEGURIDAD

La presente Política de Seguridad es administrada por BEWOR TECH S.L. en su condición de Prestador de Servicios de Electrónicos de Confianza de acuerdo a las previsiones de la Orden Ministerial ETD/465/2021 y al Anexo F.11 de la Guía de Seguridad de las TIC CCN-STIC-140, del Centro Criptológico Nacional de categoría alta. Asimismo, la misma cumple con los requisitos exigidos por el Sistema de Gestión de la Seguridad de la Información implementado por BEWOR TECH S.L.

Las modificaciones a este documento y sus correspondientes aprobaciones, se realizan a través del procedimiento de Gestión documental y si fuera necesario según lo previsto en la Política de gestión de cambios de BEWOR TECH S.L., considerando los roles y responsabilidades previstos en el proceso de toma de decisión. Igualmente, las responsabilidades sobre la implementación de la política de seguridad se asignan a través del mencionado procedimiento.

5. DEL ALCANCE Y ÁMBITO DE APLICACIÓN

Esta política de seguridad se aplicará a la ejecución de las actividades relacionadas con los servicios del Prestador de Servicios de Confianza de BEWOR TECH S.L., esto es Gestión del ciclo de vida de los certificados electrónicos (emisión, validación, mantenimiento y revocación) y microservicios (desarrollo de software compuesto por pequeños servicios independientes con comunicación a través de API). En consecuencia, la presente política será de cumplimiento obligatorio para todo el personal de BEWOR TECH S.L., y también para cualquier tercero que intervenga o participe en la ejecución de las actividades relacionadas con la prestación de dichos servicios.

6. COMUNICACIÓN

La Presente Política de Seguridad será notificada a todos los empleados, terceros y partes interesadas que participen en la ejecución de actividades relacionadas con la prestación de los servicios de confianza, de certificación y de microservicios. En la medida en que sea aplicable, será incluida dentro de los planes de formación del personal y terceros vinculados.

7. POLITICA DE PROTECCION DE DATOS PERSONALES

7.1 Principios generales

BEWOR TECH S.L. cumplirá escrupulosamente con la legislación de su jurisdicción en materia de protección de datos, la que resulte aplicable en función del tratamiento de datos personales que se lleve a cabo y la que se determine conforme a normas o acuerdos vinculantes adoptados en el seno de su empresa o, en su caso, con otros responsables del tratamiento si se tratan datos personales por cuenta de los mismos. Promoverá que los principios recogidos en esta Política de protección de datos personales sean tenidos en cuenta en el diseño e implementación de todos los procedimientos que impliquen el tratamiento de datos personales, en los servicios ofrecidos, en todos los contratos y obligaciones que formalicen con personas físicas y en la implantación de cuantos sistemas y plataformas permitan el acceso por parte de empleados o de terceros a datos personales y/o la recogida o tratamiento de dichos datos.

7.2 Principios relativos al tratamiento de datos personales

Principios de legitimidad, licitud y lealtad en el tratamiento de datos personales

El tratamiento de datos personales será leal, legítimo y lícito conforme a la legislación aplicable. En este sentido, los datos personales deberán ser recogidos para uno o varios fines específicos y legítimos conforme a la legislación aplicable.

En los casos en los que resulte obligatorio conforme a la legislación aplicable, deberá obtenerse el consentimiento de los interesados antes de recabar sus datos.

Asimismo, cuando lo exija la ley, los fines del tratamiento de datos personales serán explícitos y determinados en el momento de su recogida.

Principio de minimización

Solo serán objeto de tratamiento aquellos datos personales que resulten estrictamente necesarios para la finalidad para los que se recojan o traten y adecuados a tal finalidad.

Principio de exactitud

Los datos personales deberán ser exactos y estar actualizados. En caso contrario, deberán suprimirse o rectificarse.

Principio de limitación del plazo de conservación

Los datos personales no se conservarán más allá del plazo necesario para conseguir el fin para el cual se tratan, salvo en los supuestos previstos legalmente. Los datos personales serán suprimidos o anonimizados cuando dejen de ser necesarios para el fin o fines del tratamiento, salvo que deban ser bloqueados, en virtud de la obligación exigible al responsable del tratamiento, o conservados como consecuencia del ejercicio del derecho de limitación.

Principio de integridad y confidencialidad

En el tratamiento de los datos personales se deberá garantizar, mediante medidas técnicas u organizativas, una seguridad adecuada que los proteja del tratamiento no autorizado o ilícito y que evite su pérdida, su destrucción y que sufran daños accidentales.

Los datos personales recabados y tratados por BEWOR TECH S.L. deberán ser conservados con la máxima confidencialidad y secreto, no pudiendo ser utilizados para otros fines distintos de los que justificaron y permitieron su recogida y sin que puedan ser comunicados o cedidos a terceros fuera de los casos permitidos por la legislación aplicable.

Principio de responsabilidad proactiva (rendición de cuentas)

BEWOR TECH S.L. será responsable de cumplir con los principios estipulados en esta Política de protección de datos personales y los exigidos en la legislación aplicable y deberán ser capaces de demostrarlo, cuando así lo exija la legislación aplicable.

BEWOR TECH S.L. deberá hacer una evaluación del riesgo de los tratamientos que realicen, con el fin de determinar las medidas a aplicar para garantizar que los datos personales se tratan conforme a las exigencias legales. En los casos en los que la normativa lo exija, se evaluarán de forma previa los riesgos que para la protección de datos personales puedan comportar nuevos productos, servicios o sistemas de información y se adoptarán las medidas necesarias para eliminarlos o mitigarlos. BEWOR TECH S.L. deberá llevar un registro de actividades en el que se describan los tratamientos de datos personales que lleven a cabo en el marco de sus actividades.

En el caso de que se produzca una violación de la seguridad de los datos que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizado a dichos datos, deberán seguirse los protocolos internos establecidos a tal efecto y los que establezca la legislación aplicable. Dichas violaciones deberán documentarse y se adoptarán medidas para solventar y paliar los posibles efectos negativos para los interesados.

Principios de transparencia e información

El tratamiento de datos personales será transparente en relación con el interesado, facilitándole la información sobre el tratamiento de sus datos de forma comprensible y accesible, cuando así lo exija la normativa aplicable.

A fin de garantizar un tratamiento leal y transparente, BEWOR TECH S.L., como responsable del tratamiento deberá informar a los interesados cuyos datos se pretende recabar de las circunstancias relativas al tratamiento conforme a la legislación aplicable. Igualmente, si los datos personales no han sido obtenidos de los interesados, BEWOR TECH S.L. cumplirá con el principio de información en los términos previstos en la normativa aplicable, salvo que concurra alguna excepción al respecto o se puedan tomar otras medidas en relación con este principio.

Adquisición u obtención de datos personales

Queda prohibida la adquisición u obtención de datos personales de fuentes ilegítimas, de fuentes que no garanticen suficientemente su legítima procedencia o de fuentes cuyos datos hayan sido recabados o cedidos contraviniendo la normativa. Queda también prohibido cualquier tratamiento de datos personales que no cumpla con los requisitos exigidos en virtud de la normativa aplicable o la obtención de datos personales incumpliendo los principios de licitud y lealtad como, por ejemplo, a través de engaño o formas no permitidas por la normativa en materia de protección de datos personales.

Contratación de encargados del tratamiento

Con carácter previo a la contratación de cualquier prestador de servicios que acceda a datos personales que sean responsabilidad de BEWOR TECH S.L., así como durante la vigencia de la relación contractual, esta deberá adoptar las medidas necesarias para garantizar y, cuando sea legalmente exigible, demostrar, que el tratamiento de datos por parte del encargado se lleva a cabo conforme a la normativa aplicable.

Todo prestador de servicios que actúe como encargado del tratamiento tendrá que haber firmado o suscrito con BEWOR TECH S.L. un contrato u otro acto jurídico que cumpla con los requisitos exigidos por la normativa aplicable sobre protección de datos y deberá ser capaz, en todo momento, incluso en el momento de finalización del servicio que implique el tratamiento de datos personales, de ayudar a BEWOR TECH S.L. a cumplir y demostrar el cumplimiento en la materia.

Transferencias internacionales de datos

Todo tratamiento de datos personales que implique una transferencia de datos fuera del Espacio Económico Europeo deberá llevarse a cabo con estricto cumplimiento de los requisitos establecidos en la normativa aplicable en materia de protección de datos. Cualquier empresa o persona que reciba los datos personales como consecuencia de una transferencia internacional de datos, adoptará las medidas necesarias para cumplir con la normativa sobre protección de datos aplicable y aquellas a las que se haya obligado con BEWOR TECH S.L..

Derechos de los interesados

BEWOR TECH S.L. facilitará que los interesados puedan ejercitar los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición, incluida en su caso la elaboración de perfiles, que sean de aplicación, estableciendo, a tal efecto, medidas adecuadas y los procedimientos internos que resulten necesarios para satisfacer, al menos, los requisitos legales aplicables en cada caso.

7.3. Implementación

BEWOR TECH S.L. deberá promover una cultura proactiva de la privacidad, compromiso responsable que, a la vez, contribuya a fortalecer la protección eficaz de los derechos de las personas.

Conforme a lo dispuesto en esta Política de protección de datos personales, se desarrollará y mantendrá actualizada la normativa interna de gestión de la protección de datos, y será de obligado cumplimiento para todos los empleados/profesionales de BEWOR TECH S.L.

BEWOR TECH S.L. será responsable de reportar los desarrollos y novedades normativas que se produzcan en este ámbito. Deberá implementar en sus sistemas de información, los controles y desarrollos informáticos que sean adecuados para garantizar el cumplimiento de la normativa interna de gestión de la protección de datos y velará por que dichos desarrollos estén actualizados en cada momento.

Para ello, el sistema de gestión implantado en materia de protección de datos, seguirá el esquema siguiente:

| | |
|---|---|
| <ul style="list-style-type: none"> ▶ FASE 0. LIDERAZGO CENTRADO EN LA SEGURIDAD Y COMPROMISO DE LA POLÍTICA <ul style="list-style-type: none"> ▶ 0.1. EMPRESA-INSTITUCIÓN ▶ 0.2. Checklist- CULTURA EMPRESARIAL DE GDPR ▶ 0.3. NOMBRAMIENTOS ▶ 0.4. POLÍTICA DE PROTECCIÓN DE DATOS (ALCANCE) ▶ FASE 1. CONTEXTO DE LA ORGANIZACIÓN - ACTIVIDADES DE TRATAMIENTO DE DATOS <ul style="list-style-type: none"> ▶ 0. NORMATIVA APLICABLE ▶ 1. ASIGNACIÓN DE ROLES ▶ 2. DESCRIPCIÓN DE LA ACTIVIDAD DE TRATAMIENTO ▶ 3. TRATAMIENTO DE DATOS PERSONALES ▶ 4. TRANSFERENCIA DE DATOS PERSONALES A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES ▶ 5. REGISTROS ▶ FASE 2. EVALUACIÓN DE IMPACTO <ul style="list-style-type: none"> ▶ 1. DATOS PERSONALES ▶ 2. TRATAMIENTO ▶ 3. RESPONSABLE DEL TRATAMIENTO ▶ 4. ENCARGADO DEL TRATAMIENTO ▶ 5. FINALIDAD DEL TRATAMIENTO ▶ 6. BASES DE LEGITIMACIÓN DEL TRATAMIENTO (CONDICIONES DE LICITUD) ▶ FASE 3. GESTIÓN DE RIESGOS -AMENAZAS- MEDIDAS DE SEGURIDAD <ul style="list-style-type: none"> ▶ 3.1. Riesgos Potencialmente identificados-Amenazas ▶ 3.2. Matriz de Riesgos ▶ 3.3. Informe de riesgos ▶ 3.4. Plan de Acción-Medidas de seguridad ▶ 3.5. Catálogo de Amenazas ▶ FASE 4. MEDIDAS TÉCNICAS Y DE SEGURIDAD <ul style="list-style-type: none"> ▶ 4.1. MEDIDAS TÉCNICAS Y ORGANIZATIVAS ▶ 4.2. CÓDIGO DE CONDUCTA ▶ FASE 5. OTRAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS <ul style="list-style-type: none"> ▶ 5.1. SOLICITUD DE EJERCICIO DEL DERECHO CORRESPONDIENTE ▶ 5.2. VIOLACIONES DE SEGURIDAD DE LOS DATOS PERSONALES ▶ 5.3. SUPRESIÓN O DESTRUCCIÓN ▶ 5.4. INCIDENCIAS ▶ FASE 6. REVISIÓN Y ACTUALIZACIÓN DEL PROGRAMA <ul style="list-style-type: none"> ▶ 6.1. REVISIÓN Y ACTUALIZACIÓN DE MEDIDAS PARA EL CUMPLIMIENTO ▶ 6.2. CONSIDERACIÓN DE NUEVOS FACTORES RELATIVOS AL TRATAMIENTO DE DATOS ▶ 6.3. INDICADORES ▶ 6.4. AUDITORIA INTERNA Y CERTIFICACIÓN ▶ 6.5. FORMACIÓN Y DIVULGACIÓN ▶ FASE 7. INFORME <ul style="list-style-type: none"> ▶ Informe Evaluación Sistema de Protección de datos | <ul style="list-style-type: none"> ▶ Fase 0. LIDERAZGO CENTRADO EN LA SEGURIDAD Y COMPROMISO DE LA POLÍTICA <ul style="list-style-type: none"> ▶ 0.1. - Empresa ▶ 0.2.- Checklist - CULTURA EMPRESARIAL DE GDPR ▶ 0.3 - Designación del delegado de protección de datos ▶ 0.4 - Nombramiento del DPD ▶ 0.5. - Nombramiento Responsable de seguridad ▶ 0.6 - Política de Protección de Datos (Alcance) ▶ 0.7 - Compromiso de aprobación de Política de Protección de Datos ▶ Fase 1. CONTEXTO DE LAS ACTIVIDADES DE TRATAMIENTO DE DATOS <ul style="list-style-type: none"> ▶ 1.1 - Responsable del tratamiento ▶ 1.1.2 - Comunicaciones de datos a otros responsables ▶ 1.2 - Encargado de tratamiento <ul style="list-style-type: none"> ▶ 1.2.1 - Contrato encargado del tratamiento ▶ 1.3 - Destinatario de tratamiento ▶ 1.4 - Corresponsable del tratamiento ▶ 1.5 - Identificación del Interesado ▶ 1.6 - Usuarios Internos ▶ 1.7 - Actividad, funciones o fines ▶ 1.8 - Bases de legitimación del tratamiento ▶ 2.1 - Datos personales tratados ▶ 2.3 - Naturaleza, alcance, contexto y fines del tratamiento ▶ 2.4 - Análisis de la necesidad de realizar una evaluación de impacto <ul style="list-style-type: none"> ▶ 3.1.1 - Ficha del Registro de actividades ▶ 3.1.2 - Registro de actividades de tratamiento <ul style="list-style-type: none"> ▶ 3.1.2.1 - Inventario de datos personales Públicos ▶ 3.1.2.2 - Inventario de datos personales Privado ▶ 3.1.2.3 - Inventario de contratos con encargados del tratamiento ▶ 3.1.2.4 - Inventario de transmisiones de datos a otros responsables del tr ▶ Fase 3. GESTIÓN DE RIESGOS-AMENAZAS-MEDIDAS DE SEGURIDAD <ul style="list-style-type: none"> ▶ 3.0. - Riesgo Potencial asociado a la actividad de tratamiento <ul style="list-style-type: none"> ▶ 3.1. - Matriz de riesgo tratamiento de datos ▶ 3.3. - Informe de Riesgos ▶ 3.4. - Plan de Acción ▶ 3.5. - Catálogo de Amenazas y posibles soluciones ▶ Fase 4. MEDIDAS TÉCNICAS Y ORGANIZATIVAS <ul style="list-style-type: none"> ▶ 4.1. - Manual de medidas de seguridad Básica del Responsable del trat ▶ 4.2. - Manual de Medidas de seguridad básica del Encargado de Tratamien ▶ 4.3. - Adhesión al Código de Conducta ▶ Fase 5. OTRAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS <ul style="list-style-type: none"> ▶ 5.1. - Procedimiento de atención a derechos ▶ 5.2. - Formulario solicitud derecho de limitación del tratamiento ▶ 5.3. - Formulario solicitud derecho de rectificación ▶ 5.4. - Formulario solicitud derecho de supresión ▶ 5.5. - Formulario solicitud derecho a no ser objeto de decisiones indiv ▶ 5.6. - Formulario solicitud derecho de acceso ▶ 5.7. - Formulario solicitud derecho de oposición con fines de mercadote ▶ 5.8. - Formulario solicitud derecho de oposición ▶ 5.9. - Formulario solicitud derecho de portabilidad ▶ 6. - Registro de incidencias y notificación interna ▶ 6.1. - Comunicación a la notificación de la incidencia |
|---|---|

7.4 Control y Evaluación

Se llevará a cabo una gestión continuada de los riesgos potenciales asociados al tratamiento de datos desde su diseño.

7.4.1 Control

Corresponde a BEWOR TECH S.L., supervisar el cumplimiento de lo dispuesto en esta Política de protección de datos personales. Para verificar el cumplimiento de esta Política de protección de datos personales se realizarán auditorías periódicas con auditores internos o externos.

7.4.2 Evaluación

El Responsable de Seguridad evaluará, al menos una vez al año, el cumplimiento y la eficacia de esta Política de protección de datos personales e informará del resultado a BEWOR TECH S.L., o a la dirección que asuma dichas funciones en cada momento.

El Delegado de Protección de Datos o a la dirección que asuma sus funciones, en caso de que el primero no hubiera sido nombrado, evaluará, al menos una vez al año o cada vez que sea necesario en atención al riesgo que implique el tratamiento de datos personales, el cumplimiento y la eficacia de esta Política de protección de datos personales y pondrá en conocimiento de BEWOR TECH S.L. el resultado de dicha evaluación.

Todos los derechos están reservados. Ninguna parte de este documento puede ser ni reproducido ni transmitido de ninguna manera, o almacenado en un sistema recuperable, o por otros medios, mecánico, fotográfico, eléctrico, electrónico, o de otro modo sin el permiso explícito de Bewor Tech S.L.

All rights reserved. No part of this publication may be reproduced, transmitted in any form, or stored in a retrieval system, or by any means, mechanical, photographic, electrical, electronic, or otherwise without the express permission of Bewor Tech S.L.