Barrabés

Política de Seguridad de la Información

ISO 27001

Esquema Nacional de Seguridad

Versión 2.0

Política

La misión de Barrabés.biz es acompañar durante todo el proceso de innovación, desde la identificación de retos hasta el lanzamiento en el mercado, para adaptar los negocios a un mundo en constante cambio, guiado por un propósito que cree beneficios a nuestros clientes, a la sociedad y al planeta.

La Política de Seguridad de Barrabés.biz refleja los principios y objetivos en materia de seguridad de la información, cuyos resultados permiten a nuestra empresa alcanzar su propósito de aumentar las ventas de nuestros clientes mediante la captación, generación y control de calidad de leads.

Mediante la elaboración, comunicación y mantenimiento de esta política, la Dirección de Barrabés.biz muestra su compromiso de proteger la **confidencialidad** de la información con la que opera en la prestación de sus servicios, garantizar su **integridad** en todos los procesos de tratamiento que lleve a cabo, así como la **disponibilidad** de los sistemas de información implicados en estos tratamientos.

Para ello, la Dirección ha definido e implantado un Sistema de Gestión de la Seguridad de la Información que permite a la compañía garantizar que los sistemas de información y la información que se crea, recopila, almacena y procesa cumple con:

- La seguridad en la Gestión de los Recursos Humanos, antes, durante y al finalizar la relación laboral.
- La gestión adecuada de los activos que implique la clasificación de la información y la manipulación de los soportes, y el establecimiento de un robusto control de acceso lógico a sus sistemas y aplicaciones, gestionando los permisos y los privilegios de los usuarios.
- La protección de las instalaciones y del entorno físico, mediante el diseño de áreas de trabajo seguras y la seguridad de los equipos.
- La garantía de la seguridad en las operaciones mediante la protección contra el software malicioso, la realización de copias de seguridad, el establecimiento de registros y su supervisión. el control del software en explotación.
- La gestión de las vulnerabilidades técnicas y la elección de técnicas adecuadas para la auditoria de los Sistemas.
- La seguridad de las comunicaciones, protegiendo las redes y el intercambio de Información.
- El aseguramiento de la seguridad en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.
- La realización de un desarrollo seguro de software, separando los entornos de desarrollo y producción, y realizando las pruebas funcionales de aceptación adecuadas.

- El control de las relaciones con los proveedores, exigiendo de forma contractual el cumplimiento de las medidas de seguridad pertinentes y unos niveles aceptables en sus servicios.
- La eficacia en la gestión de los incidentes de seguridad, estableciendo los canales adecuados para su notificación, respuesta y aprendizaje oportuno.
- La realización de un plan de continuidad de negocio que proteja la disponibilidad de los servicios durante una crisis o desastre.
- La identificación y cumplimiento de la normativa aplicable poniendo especial interés en la propiedad intelectual y en la protección de los datos de carácter personal.
- La revisión periódica y mejora continua de nuestro sistema de gestión de la seguridad de la información para garantizar el cumplimiento y eficacia de estos requisitos.

El marco legal y regulatorio en el que desarrollamos nuestras actividades es:

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual
- Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual
- Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Para el cumplimiento de la presente política se designan las siguientes funciones:

El **responsable de la información** será el propietario de esta y tendrá las siguientes funciones;

- Clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad), dentro del marco del ENS.
- Trabajar en colaboración con el responsable de seguridad y el del sistema en el mantenimiento de los servicios de administración catalogados.

- Apoyar la realización de los análisis de riesgos y valorar las diferentes opciones de gestión del riesgo a implantar.
- Valorar y decidir, junto con el responsable del Servicio, los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes que puedan tener acceso a información de los procedimientos administrativos que gestiona y realizar el seguimiento de su cumplimiento.

El **responsable del servicio** será quien determine los requisitos de los servicios prestados, en consonancia, tendrá las siguientes funciones:

- Establecer los requisitos del servicio en materia de seguridad, o, en terminología del ENS, la protestad de determinar los niveles de seguridad de los servicios.
- Clasificar los servicios conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), dentro del marco establecido en el Anexo I del ENS.
- Atender a los requisitos de seguridad de la información, tales como disponibilidad, accesibilidad, interoperabilidad que se demanden en la prestación de los servicios.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes que puedan afectar a sus servicios y realizar el seguimiento de su cumplimiento.

El **responsable de seguridad** será quien tome las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios. Dispondrá de las siguientes funciones:

- Supervisar el cumplimiento de la presente Política, de sus normas y procedimientos derivados.
- Asesorar en materia de seguridad a los integrantes Comité de Seguridad que así lo requieran.
- Coordinar la interacción con otros organismos especializados.
- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
- Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
- Asesorar, en colaboración con los responsables de los Sistemas, los responsables de los Servicios y de la Información, en la realización del análisis y gestión de riesgos, elevando el informe resultante al Comité de Seguridad.

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones Comité de Seguridad en materia de seguridad.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
- Elaboración y revisión de la normativa de seguridad Comité de Seguridad.
- Aprobación de los procedimientos de seguridad elaborados por el responsable del Sistema.

El **responsable de los sistemas de información**, dentro de sus áreas de actuación, tendrán asignadas las siguientes funciones:

- Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Elaborar procedimientos técnicos de seguridad de los sistemas de información.
- Elaborar planes de continuidad de los sistemas de información.
- Colaborar para la realización del análisis de riesgos de los sistemas de información de los que es responsable.
- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.

Para coordinar la implantación del sistema se define un Comité de Seguridad ENS. El comité de seguridad ENS es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información para ENS y está formado por el responsable de la información, el responsable del servicio, el responsable de seguridad y el responsable de los sistemas de información. La toma de decisiones se realizará mediante la votación de los miembros y con el único requisito de mayoría simple. En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad.

La gestión de la seguridad ENS se encomienda al responsable de seguridad que informará al comité de seguridad ENS de las necesidades de la emisión de políticas y procedimientos complementarios a las políticas de seguridad corporativa para asegurar el cumplimiento de la normativa española.

Estos miembros se designan por el Comité de dirección, único órgano que puede nombrarlos, renovarlos y cesarlos.

La estructura de nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:

- Procedimientos
- Políticas
- Normas y códigos

Todo el personal de la organización tiene el deber de acatar esta política, para lo cual la Dirección dispone los medios necesarios y recursos suficientes para su cumplimiento, y asume la responsabilidad de comunicarla y mantenerla accesible a todas las partes interesadas.

73197351N JUAN CARLOS BARRABES (R: B86413689)

Firmado digitalmente por 73197351N JUAN CARLOS BARRABES (R: B86413689)

Madrid, 25 de mayo de 2022