



POLITICA DE SEGURIDAD PARA EMPRESAS PROVEEDORAS

© Izenpe 2024

Este documento es propiedad de Izenpe. Únicamente puede ser reproducido en su totalidad.

■ Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.eus
izenpe@izenpe.eus



Histórico de versiones:

VERSIÓN	FECHA	CAMBIOS
1.0	10/11/2016	Versión inicial
1.1	03/02/2020	<ol style="list-style-type: none">1. Eliminado el tipo de servicio por lugar en apartado 3.12. Añadido el tipo de usuario “punto de identificación” en apartado 3.13. Modificada la clasificación del tipo de servicio ofrecido en el apartado de políticas específicas
1.2	15/03/2022	<ol style="list-style-type: none">4. Revisión completa y actualización punto 1.A Propósito; 2.1. Prestación de servicios a Izenpe. Añadido criticidad y gestión de empresa proveedoras según criticidad.
1.3	29/03/2023	<ol style="list-style-type: none">5. Ciclo de vida del documento, referencias normativas, e instrucciones a la finalización del contrato.
1.4	27/12/2023	<ol style="list-style-type: none">6. Se modifica el apartado “Referencias”



Índice

1.	INTRODUCCIÓN.....	4
1.1.	PROPÓSITO	4
1.2.	ÁMBITO DE APLICACIÓN	4
1.3.	CICLO DE VIDA DEL DOCUMENTO	4
2.	REFERENCIAS.....	5
3.	POLÍTICAS DE SEGURIDAD GENERALES	5
3.1.	PRESTACIÓN DE SERVICIOS A IZENPE	5
3.2.	CONFIDENCIALIDAD DE LA INFORMACIÓN.....	6
3.3.	PROPIEDAD INTELECTUAL.....	7
3.4.	INTERCAMBIO DE INFORMACIÓN.....	7
3.5.	USO APROPIADO DE LOS RECURSOS	8
3.6.	RESPONSABILIDADES DE LA PERSONA USUARIA	9
3.7.	EQUIPOS DE PERSONAS USUARIAS.....	11
4.	POLÍTICAS DE SEGURIDAD ESPECÍFICAS	11
4.1.	APLICABILIDAD DE LAS POLÍTICAS DE SEGURIDAD ESPECÍFICAS PARA EMPRESA PROVEEDORAS.....	11
4.1.1.	Tipos de empresa proveedora:	12
4.1.2.	Criticidad de las empresas proveedoras:.....	12
4.1.3.	Gestión de las empresas proveedoras según criticidad	14
4.2.	SELECCIÓN DE PERSONAL	14
4.3.	AUDITORÍA DE SEGURIDAD	14
4.4.	COMUNICACIÓN DE INCIDENCIAS.....	14
4.5.	SEGURIDAD FÍSICA.....	15
4.6.	GESTIÓN DE ACTIVOS	16
4.7.	ARQUITECTURA DE SEGURIDAD.....	16
4.8.	SEGURIDAD DE SISTEMAS.....	16
4.9.	SEGURIDAD DE RED	18
4.10.	TRAZABILIDAD DE USO DE LOS SISTEMAS	19
4.11.	CONTROL Y GESTIÓN DE IDENTIDADES Y ACCESOS.....	19
4.12.	GESTIÓN DE CAMBIOS.....	20
4.13.	SEGURIDAD EN DESARROLLO	20
4.14.	GESTIÓN DE CONTINGENCIAS	21
4.15.	FINALIZACIÓN DEL CONTRATO SUSCRITO CON IZENPE	22
5.	SEGUIMIENTO Y CONTROL	22
6.	ACTUALIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD	22



1. INTRODUCCIÓN

1.1. PROPÓSITO

El objetivo de este documento es establecer las directrices garantes de la seguridad de la información aplicables a las entidades proveedoras de *Ziurtapen eta Zerbitzu Enpresa-Entidad de Certificación y Servicios, Izenpe S.A.* (en adelante Izenpe).

Su finalidad es evitar posibles pérdidas o usos indebidos, deterioro o indisponibilidad de los sistemas de información que pueda dañar o perjudicar al servicio que ofrece o a la reputación de Izenpe, pudiendo interrumpir el normal desarrollo de la operativa, produciendo efectos negativos en la calidad del servicio y los beneficios de la compañía. Para ello esta Política describe los requisitos aplicables a las entidades proveedoras, que en el desarrollo de sus funciones pudieran tener acceso a información o recursos de Izenpe.

El principal objetivo es mitigar los riesgos asociados a los sistemas de información de la empresa, describiendo lo que se espera de todo el personal que pertenece a otras empresas proveedoras que trabajan para Izenpe y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos en general, con el fin de proteger la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y sistemas manejados por Izenpe.

Para ello, las entidades proveedoras se responsabilizarán de que las personas que trabajen para Izenpe conozcan y se comprometan por escrito a respetar esta Política.

Este documento se considera de uso interno y, por lo tanto, no podrá ser divulgado salvo autorización de Izenpe.

1.2. ÁMBITO DE APLICACIÓN

Esta Política será de aplicación a todas las actividades desarrolladas por personal de entidades proveedoras que tengan acceso, traten información de Izenpe, o que realicen desarrollos para Izenpe, vinculadas a través del correspondiente marco contractual.

Será aplicable a cualquier empresa proveedora (en el ámbito indicado anteriormente), independientemente del tipo de servicio proporcionado.

Cada uno de los sub-apartados del apartado "POLÍTICAS DE SEGURIDAD ESPECÍFICAS" de la presente política será aplicable exclusivamente a aquella empresa proveedora cuyos servicios proporcionados se correspondan con el tipo de servicio indicado en cada caso, tal y como se indica al comienzo del citado apartado.

1.3. CICLO DE VIDA DEL DOCUMENTO

La presente Política entrará en vigor al día siguiente de la fecha de aprobación (fecha efectiva) por el Comité de Seguridad. La nueva versión en vigor de cada documento reemplaza de forma inmediata a la anterior, que pasará al estado de retirado.

La política se revisará en caso de necesidad para adaptarla a las condiciones cambiantes del negocio, el entorno tecnológico y a las nuevas amenazas o en su defecto anualmente como máximo.



2. REFERENCIAS

- Política de Seguridad de la Información de Izenpe.
- Esquema Nacional de Seguridad - ENS

3. POLÍTICAS DE SEGURIDAD GENERALES

3.1. PRESTACIÓN DE SERVICIOS A IZENPE

1. La actividad desarrollada por la entidad proveedora se realizará de acuerdo a lo establecido en el correspondiente marco regulador, así como a las normas y procedimientos establecidos a tal efecto entre Izenpe y la empresa proveedora.
2. La entidad proveedora proporcionará a Izenpe al comienzo la relación de personas, perfiles, funciones y responsabilidades asociados al servicio provisto e informará puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.
3. De acuerdo a lo establecido en el instrumento regulador todo el personal externo que desarrolle labores para Izenpe deberá cumplir con lo determinado en este documento. La empresa proveedora adoptará las medidas necesarias y garantizará (mediante formación, mensajes de concienciación, etc.) que toda persona relacionada con el servicio prestado conoce, y cumple con las políticas y medidas de seguridad exigidas por Izenpe en el correspondiente instrumento reguladores. Éstos deberán estar informados de forma comprensible de la existencia del mismo, de las normas de seguridad que afectan al desarrollo de sus funciones, las consecuencias en caso de incumplimiento y el carácter confidencial de la Información, subsistiendo la obligación de confidencialidad aún finalizada la relación laboral con la empresa proveedora.

Las personas que desempeñan funciones profesionales deben ser conscientes de la importancia de la información de Izenpe, tratar la misma de forma segura y estar formadas y cualificadas en todas y cada una de las fases de proceso de la información, para todas y cada una de las funciones que desempeñen. Las personas usuarias deberán observar toda la diligencia posible y medidas adecuadas para proteger el proceso de la información en cumplimiento de su deber de buena fe a la que están obligados contractualmente. El representante legal de la empresa proveedora comunicará a sus empleados la Política de Seguridad de Izenpe, debiendo firmarla.

En caso de incumplimiento, Izenpe se reserva el derecho de veto sobre el personal que haya cometido la infracción, así como la adopción de las medidas sancionadoras que se consideren pertinentes en relación a la entidad contratada, y que pueden llegar a la resolución de los acuerdos vigentes.

4. La entidad proveedora deberá asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio prestado, tanto a nivel específico en las materias correspondientes a la actividad asociada a la prestación del servicio como de manera transversal en materia de seguridad de la información, para lo cual deberá asegurarse de que todo el personal asociado al servicio conoce y se compromete a cumplir esta *Política*.



5. Cualquier tipo de intercambio de información que se produzca entre Izenpe y las entidades proveedoras se entenderá realizado dentro del marco contractual existente entre ambas partes de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho acuerdo.
6. El *Área de Seguridad de la Información* centraliza los esfuerzos globales de protección de los activos de Izenpe, a fin de asegurar el correcto funcionamiento de las tecnologías de la información que soportan los procesos de la organización.

3.2. CONFIDENCIALIDAD DE LA INFORMACIÓN

La confidencialidad de la información se define como la garantía de que la información no sea divulgada de forma inadecuada a otras entidades o procesos. Con el fin de preservarla:

1. El personal externo que tenga acceso a información de Izenpe deberá considerar que dicha información, por defecto, tiene el carácter de confidencial.

Sólo se podrá considerar como información no confidencial aquella información de Izenpe a la que haya tenido acceso a través de los medios de difusión pública de información.

2. Se evitará la revelación, modificación, destrucción o mal uso de la información cualquiera que sea el soporte en que se encuentre contenida.
3. Se guardará por tiempo indefinido la máxima reserva, salvo autorización expresa.
4. Se minimizará el número de informes en formato papel que contengan información confidencial y se mantendrán en lugar seguro y fuera del alcance de terceros.
5. El personal externo únicamente utilizará las herramientas dispuestas por Izenpe o por la entidad proveedora, y en cualquier caso exclusivamente para usos profesionales.
6. Ningún colaborador deberá poseer para usos no propios de su responsabilidad, ningún material o información propia o confiada a Izenpe.
7. En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la entidad proveedora acceda a información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicho acceso es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.

Asimismo, el empleado deberá devolver el/los soportes inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación de su entidad con Izenpe.

La utilización continuada de la información en cualquier formato o soporte distinto al pactado y sin conocimiento de Izenpe no supondrá, en ningún caso, una modificación de este punto.

8. Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para Izenpe.
9. El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en el artículo 197 del Código Penal, que puede dar derecho a exigir compensaciones.



10. El personal sólo podrá crear ficheros temporales que contengan datos de carácter personal cuando sea necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de los puestos PC del personal y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.
11. La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicada dicha información deberá ser autorizada por Izenpe y se realizará según el procedimiento definido. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar de acceso restringido al personal autorizado.
12. La información sobre todos los tratamientos de datos personales de Izenpe están disponibles en www.izenpe.eus/datos.

3.3. PROPIEDAD INTELECTUAL

1. Las entidades externas que acceden a Internet a partir de la red informática y terminales corporativos serán responsables de respetar los derechos de propiedad intelectual aplicables a los contenidos accedidos.
2. Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.
3. Las personas usuarias externas únicamente podrán utilizar material autorizado por su empresa o por Izenpe para el desarrollo de sus funciones.
4. Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización.

3.4. INTERCAMBIO DE INFORMACIÓN

1. Ninguna persona debe ocultar o manipular su identidad bajo ninguna circunstancia.
2. La distribución de información, en soporte digital o en papel se realizará con la finalidad exclusiva de facilitar las funciones asociadas a dicho acuerdo. Izenpe se reserva, en función del riesgo identificado, la implementación de medidas adicionales de control, registro y auditoría.
3. En relación al intercambio de información dentro del marco contractual existente entre las partes, se considerarán no autorizadas las siguientes actividades:
 - a) Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.
 - b) Transmisión o recepción de mensajes de naturaleza sexual, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
 - c) Transferencia de ficheros a terceras partes no autorizadas de material de la organización o material que sea de alguna u otra manera confidencial.



- d) Transmisión o recepción de ficheros que infrinjan la normativa de protección de datos de carácter personal.
 - e) Transmisión o recepción de aplicaciones no relacionadas con el negocio.
 - f) Participación en actividades de Internet que no estén directamente relacionadas con el servicio.
 - g) Todas las actividades que puedan dañar la buena reputación de Izenpe están prohibidas.
4. Si el tratamiento de datos de carácter personal se llevase a cabo fuera de los locales de Izenpe, deberá garantizarse el nivel de seguridad correspondiente al tipo de tratamiento.
5. La transmisión de datos de carácter personal categorizados como especialmente protegidos según el Reglamento Europeo 2016/679 de tratamiento de datos personales, se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

3.5. USO APROPIADO DE LOS RECURSOS

1. La empresa proveedora se compromete a utilizar los recursos dispuestos para la provisión del servicio de acuerdo a las condiciones para las que fueron diseñados e implantados.
2. Los recursos que Izenpe pone a disposición del personal externo, (informáticos, datos, software, redes, sistemas de comunicación, etc.), estarán disponibles exclusivamente para el cumplimiento de las obligaciones y propósito de la operativa para la que fueron proporcionados. Izenpe se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.
3. Todos los equipos de la empresa proveedora que se conecten a la red corporativa de Izenpe (físicamente o por VPN) deberán estar homologados. La empresa proveedora pondrá a disposición de Izenpe dichos equipos para que Izenpe instale el software homologado y se configuren adecuadamente.
4. Cualquier fichero introducido en la red corporativa de Izenpe o en cualquier equipo conectado a ella a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.
5. Al finalizar la relación se deberá eliminar toda la información y software proporcionados por Izenpe, sin retraso justificado.
6. Se prohíbe expresamente:
 - a. El uso de los recursos proporcionados por Izenpe para actividades no relacionadas con el propósito del servicio.
 - b. La conexión a la red corporativa de Izenpe (físicamente o por VPN) de equipos y/o aplicaciones que no estén especificados como parte del software propios de Izenpe o bajo su supervisión.
 - c. Introducir voluntariamente en la red de Izenpe cualquier tipo de malware (programas, macros, applets, controles ActiveX, etc.), dispositivo lógico, dispositivo



físico o cualquier otro tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos. Intentar obtener sin autorización explícita otros derechos o accesos distintos a aquellos que Izenpe les haya asignado.

- d. Intentar acceder sin autorización explícita a áreas restringidas de los Sistemas de Información de Izenpe.
- e. Intentar distorsionar o falsear los registros “log” de los Sistemas de Información de Izenpe.
- f. Intentar descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de Izenpe.
- g. Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otras personas usuarias, ni dañar o alterar los recursos informáticos de Izenpe.
- h. Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos responsabilidad de Izenpe.

3.6. RESPONSABILIDADES DE LA PERSONA USUARIA

1. Las empresas proveedoras de servicios deberán asegurar que el personal que desarrolla labores para Izenpe respete los siguientes principios básicos dentro de su actividad informática:
 - a) Cada persona con acceso a información de Izenpe es responsable de la actividad desarrollada por su identificador de persona usuaria y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control sus credenciales.
 - b) Las personas usuarias no deberán utilizar ningún identificador de otra persona usuaria, aunque dispongan de la autorización de la persona propietaria.
 - c) Las personas usuarias conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.
2. Cualquier persona con acceso a información responsabilidad de Izenpe deberá seguir las siguientes directrices en relación a la gestión de las contraseñas:
 - a) Seleccionar contraseñas de calidad.
 - b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
 - c) Cambiar las contraseñas periódicamente y evitar reutilizar o reciclar viejas contraseñas.
 - d) Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión (“login”).
 - e) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.



- f) Notificar cualquier incidente de seguridad relacionado con sus contraseñas como pérdida, robo o indicio de pérdida de confidencialidad.
- 3. Cualquier persona usuaria autorizado a acceder a información responsabilidad de Izenpe deberá velar porque los equipos queden protegidos cuando vayan a quedar desatendidos.
- 4. Cualquier persona con acceso a información responsabilidad de Izenpe deberá respetar al menos las políticas de escritorio limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.
- 5. Almacenar bajo llave los documentos en papel y los medios informáticos que contengan información responsabilidad de Izenpe en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
 - a) No dejar desatendidos los equipos asignados a funciones críticas de Izenpe y bloquear su acceso.
 - b) Proteger, tanto los puntos de recepción y envío de información (correo postal, máquinas de escaner y fax) como los equipos de duplicado (fotocopiadora, fax y escaner). La reproducción o envío de información con este tipo de dispositivos quedará bajo la responsabilidad de la persona usuaria.
 - c) Retirar, sin retraso injustificado, cualquier información confidencial o con datos de carácter personal, una vez impresa.
 - d) Los listados con datos de carácter personal o información confidencial deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.
 - e) Los listados con datos de carácter personal o información confidencial deberán eliminarse de manera segura una vez no sean necesarios.
 - f) Las personas con acceso a sistemas y/o información nunca deberán sin autorización explícita, realizar pruebas para detectar y/o utilizar una supuesta debilidad o incidente de seguridad.
 - g) Ninguna persona intentará sin autorización explícita ni por ningún medio, transgredir el sistema de seguridad y las autorizaciones. Se prohíbe la captura de tráfico de red por parte de las personas usuarias, salvo que se estén llevando a cabo tareas de auditoría expresamente autorizadas.
 - h) Ningún dato de carácter personal será almacenado en equipos de persona usuaria ni soportes de información, excepto previa autorización expresa de Izenpe.
- 6. Todo el personal que acceda a la información y/o los sistemas responsabilidad de Izenpe deberá seguir las siguientes normas de actuación:
 - a) Proteger la información confidencial perteneciente o cedida por terceros a Izenpe de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
 - b) Contar con la autorización necesaria para obtener el acceso a los sistemas de información y/o la información accedidos.



- c) Conocer, aceptar y cumplir esta Política antes de acceder a la información y/o los sistemas de Izenpe.
7. Ninguna persona usuaria recibirá un identificador de acceso a los sistemas de Izenpe hasta que no acepte formalmente la Política de Seguridad vigente.

3.7. EQUIPOS DE PERSONAS USUARIAS

1. Las empresas proveedoras de servicios deberán asegurarse de que todo el equipamiento informático de la persona usuaria utilizado para acceder a información responsabilidad de Izenpe cumple las siguientes políticas:
 - a) Cuando se desatienda un puesto durante un periodo largo de tiempo el sistema deberá activar su bloqueo.
 - b) Ningún equipo dispondrá de herramientas que puedan transgredir el sistema de seguridad y las autorizaciones dentro de los sistemas de la organización.
 - c) Los equipos se mantendrán de acuerdo a las especificaciones del fabricante.
 - d) Todos los equipos están adecuadamente protegidos frente a malware.
 - e) Se establecerá una actualización automática de los ficheros de definición de virus.
 - f) Se establecerá una política de actualizaciones de seguridad que exigirá al menos una frecuencia mensual de consulta e instalación de dichas actualizaciones.
2. Se velará especialmente por la seguridad de todos los equipos portátiles que contengan información responsabilidad de Izenpe o permitan acceder a ella de algún modo:
 - a) Verificando que no incluyen más información que la que sea estrictamente necesaria.
 - b) Garantizando que se aplican controles de acceso a dicha información.
 - c) Minimizando los accesos a dicha información en presencia de personas ajenas al servicio provisto a Izenpe.
 - d) Transportando los equipos en fundas, maletines o equipamiento similar que incorpore la apropiada protección frente a golpes.
 - e) Tomando especiales precauciones en el exterior de las dependencias de la empresa proveedora para evitar la visión accidental por parte de terceras personas.

4. POLÍTICAS DE SEGURIDAD ESPECÍFICAS

4.1. APLICABILIDAD DE LAS POLÍTICAS DE SEGURIDAD ESPECÍFICAS PARA EMPRESA PROVEEDORAS

Todas las empresas proveedoras deberán cumplir, además de las políticas generales de seguridad para empresas proveedoras, las políticas específicas de seguridad recogidas en el presente apartado que les correspondan en cada caso, en función del nivel de acceso a los sistemas de información, y de las características del servicio prestado.



4.1.1. Tipos de empresa proveedora:

- **Sin acceso a sistemas:** el servicio provisto no requiere de la utilización de los sistemas de información de Izenpe, de modo que el personal que presta el servicio no dispone de cuentas de persona usuaria en dichos sistemas.
- **Puesto de identificación (aplicación Impresos o equivalente):** el servicio prestado consiste en la identificación y registro de solicitantes de medios de identificación (ej: certificado ciudadano, BAKQ, etc.). El personal que presta el servicio dispone de cuentas de persona usuaria que les permiten acceder a las aplicaciones de registro. Es un caso especial de operador remoto de aplicaciones de Izenpe.
- **Operador remoto de aplicaciones de Izenpe (ej: Archivo, Administración, etc.):** el servicio prestado requiere de la utilización de los sistemas de información de Izenpe de modo que el personal que presta el servicio dispone de cuentas de persona usuaria que les permiten acceder de forma remota (no se requiere el acceso a la red corporativa) a las aplicaciones de Izenpe.
- **Con acceso a red corporativa con nivel persona usuaria:** el servicio prestado requiere el acceso a través de la red corporativa (físicamente o por VPN) a alguno de los sistemas de información de Izenpe con privilegios de persona usuaria.
- **Con acceso a red corporativa con nivel privilegiado (ej: albergues):** el servicio prestado requiere del acceso privilegiado a los sistemas de información de Izenpe, con capacidad para administrar dichos sistemas y/o los datos de producción que procesan.

4.1.2. Criticidad de las empresas proveedoras:

El nivel de criticidad de la empresa proveedora será asignado al nivel más restrictivo:

Crítico:

- Empresa proveedora con actividad de administración en sistemas relevantes.
- Acceso a información clasificada como confidencial.
- Sistemas informáticos o servicios cloud que gestionen procesos relevantes o información clasificada como confidencial o afectada por regulaciones específicas.

Alto:

- Empresa proveedora con actividad de desarrollo sistemas relevantes o administración en sistemas no relevantes.
- Acceso a información clasificada como restringida.
- Sistemas informáticos o servicios cloud que gestionen procesos relevantes o información restringida.

Medio:

- Empresa proveedora con actividad de desarrollo en sistemas no relevantes.
- Acceso a información clasificada como interna.
- Sistemas informáticos o servicios cloud que gestionen procesos relevantes o información interna.



- Empresa proveedoras que realicen su actividad de forma remota sin acceso a información restringida.

Bajo:

- Cualquier empresa proveedora no catalogado en los niveles anteriores y cuyo desempeño en los servicios de Izenpe no implique riesgo relevante

En función de cada una de las categorías en las que se encuadre cada servicio, la empresa proveedora deberá cumplir, adicionalmente a las políticas generales de seguridad, las políticas específicas recogidas en los apartados que se indican en la siguiente tabla:

	Sin acceso a sistemas	Puesto identificación	Operador remoto aplicaciones	Acceso red corporativa a nivel persona usuaria	Acceso red corporativa a nivel privilegiado
Selección de personal	SI	SI	SI	SI	SI
Auditoría de seguridad	SI	SI	SI	SI	SI
Comunicación de incidencias	SI	SI	SI	SI	SI
Seguridad física	NO	NO	SI	SI	SI (1)
Gestión de activos	NO	NO	NO	SI	SI
Arquitectura de seguridad	NO	NO	NO	NO	SI (1)
Seguridad de sistemas	NO	NO	SI	SI	SI
Seguridad de red	NO	NO	NO	SI	SI
Trazabilidad de uso de los sistemas	NO	NO	NO	NO	SI (1)
Control y gestión de identidades y accesos	NO	NO	NO	NO	SI (1)
Gestión cambios	NO	NO	NO	NO	SI (1)
Seguridad en desarrollo	NO	NO	NO	SI(2)	SI(2)
Gestión contingencias	NO	NO	NO	NO	SI (3)

(1) Sólo si se alberga o se presta el servicio mediante su propia infraestructura TIC

(2) Sólo si existen tareas de desarrollo

(3) Sólo si se ofrecen servicios considerados críticos en el Plan de Continuidad de Negocio de Izenpe



4.1.3. Gestión de las empresas proveedoras según criticidad

Riesgo bajo: es aceptado

Riesgo medio: supervisión de medidas de seguridad, medidas específicas sobre la información confidencial. Supervisión del cumplimiento de las políticas de Izenpe, NDA y certificación de seguridad (ISO 27001, ENS, ISO 22301) de supervisor externo.

Riesgo alto y crítico: supervisión de medidas de seguridad, medidas específicas sobre la información confidencial. Supervisión del cumplimiento de las políticas de Izenpe, NDA y certificación de seguridad (ISO 27001, ENS, ISO 22301) de supervisor externo.

La gestión de las personas usuarias, equipamiento TI, accesos a servicios, etc. para el personal de empresa proveedora externo contemplará las medidas técnicas individuales reflejadas en este procedimiento. Además, se deberán incluir las cláusulas de seguridad en los contratos definidas en el Anexo I.

4.2. SELECCIÓN DE PERSONAL

Las empresas proveedoras de Izenpe que requieran acceder a los sistemas de información de Izenpe deberán cumplir las siguientes políticas de selección de personal:

1. Deberán verificar los antecedentes profesionales del personal, garantizando a Izenpe que en el pasado no ha sido sancionado por mala praxis profesional ni haya estado vinculado con incidentes relacionados con la confidencialidad de la información tratada y que le hayan supuesto algún tipo de sanción.
2. Garantizar a Izenpe la posibilidad de baja inmediata del personal asignado al servicio.

4.3. AUDITORÍA DE SEGURIDAD

Todas las empresas proveedoras de servicios que requieran acceder a los sistemas de información de Izenpe deberán cumplir las siguientes políticas de auditoría de seguridad:

1. La empresa proveedora deberá permitir a Izenpe llevar a cabo al menos una auditoría de seguridad del servicio al año, colaborando con el equipo auditor y facilitando todas las evidencias y registros requeridos.
2. El alcance y profundidad de cada auditoría será establecido expresamente por Izenpe en cada caso. Las auditorías se llevarán a cabo siguiendo la planificación que se acuerde en cada caso con la empresa proveedora del servicio.
3. Izenpe se reserva el derecho de realizar auditorías extraordinarias adicionales, siempre que se den causas específicas que lo justifiquen.

4.4. COMUNICACIÓN DE INCIDENCIAS

Todas las empresas proveedoras de servicios que accedan (tanto privilegiado como no privilegiado) a los sistemas de información de Izenpe deberán cumplir las siguientes políticas de comunicación de incidencias:



1. Todas las personas asignadas al servicio deberán ponerse en contacto con el CAU de Izenpe en caso de que detecte cualquier incidencia relacionada con la seguridad de la información o los recursos de Izenpe.
2. Cualquier persona usuaria podrá trasladar a la persona Responsable de Seguridad de Izenpe sugerencias, debilidades, vulnerabilidades y/o situaciones de riesgo que pueda tener relación con la seguridad de la información y las directrices contempladas en las presentes políticas de las que tenga conocimiento.
3. Se deberá notificar al CAU de Izenpe cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal.
4. Si no se tuviera acceso al CAU, se deberán utilizar los cauces de comunicación establecidos dentro del propio servicio, de modo que sea la interlocutora de Izenpe quien se ponga en contacto con el CAU.

4.5. SEGURIDAD FÍSICA

Todas las empresas proveedoras que presten los servicios desde la sede de la empresa proveedora deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad física:

- a) La sede deberá ser una sede cerrada y deberá contar con algún sistema de control de acceso que garantice la prevención ante robo, destrucción o interrupción del servicio.
 - b) Existirá algún tipo de control de las visitas, al menos en áreas de acceso público y/o de carga y descarga.
 - c) La sede deberá contar, al menos, con sistemas de detección de incendios, y deberá estar construida de modo que ofrezca una suficiente resistencia frente a inundaciones.
 - d) Si se mantiene algún tipo de copia de información responsabilidad de Izenpe, los sistemas que alberguen y/o procesen dicha información deberán estar ubicados en un área especialmente protegida, que incluya al menos las siguientes medidas de seguridad:
1. El área especialmente protegida deberá tener un sistema de control de acceso independiente al de la sede.
 2. Se limitará el acceso al personal externo a las áreas especialmente protegidas. Este acceso se asignará únicamente cuando sea necesario y se encuentre autorizado, y siempre bajo la vigilancia de personal autorizado.
 3. Se mantendrá un registro de todos los accesos de personas ajenas.
 4. El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.
 5. El consumo de alimentos o bebidas en estas áreas especialmente protegidas estará prohibido.
 6. Los sistemas ubicados en estas áreas deberán contar con algún tipo de protección frente a fallos de alimentación.



4.6. GESTIÓN DE ACTIVOS

Todas las empresas proveedoras de servicios que presten el servicio mediante su propia infraestructura TIC deberán garantizar que se cumplen, al menos, las siguientes políticas de gestión de activos:

1. Contar con un registro de activos actualizado en el que se puedan identificar los activos utilizados para la prestación del servicio.
2. Todos los activos utilizados para la prestación del servicio deberán tener una persona responsable, que deberá asegurar que dichos activos incorporan las medidas de seguridad mínimas establecidas por la organización, y que al menos deben ser las especificadas en la presente Política.
3. Siempre que un activo haya contenido información responsabilidad de Izenpe, la empresa proveedora deberá llevar a cabo las bajas de activos garantizando la eliminación segura de dicha información, aplicando funciones de borrado seguro o destruyendo físicamente el activo, para que la información que haya contenido no pueda ser recuperable.

4.7. ARQUITECTURA DE SEGURIDAD

Todas las empresas proveedoras de servicios que accedan a los sistemas de información de Izenpe y que presten el servicio mediante su propia infraestructura TIC, deberán garantizar que se cumplen, al menos, los siguientes requisitos de arquitectura de seguridad:

- a) Todos los accesos a los sistemas de información que alberguen o procesen información responsabilidad de Izenpe deberán estar protegidos, al menos, por un firewall que limite la capacidad de conexión a ellos.
- b) Los sistemas de información que alberguen o procesen información responsabilidad de Izenpe especialmente sensible deberán estar aislados del resto.
- c) Los sistemas de información utilizados para la prestación de servicios deberán contar con la redundancia suficiente para satisfacer los requisitos de disponibilidad.
- d) Los relojes de los sistemas de la empresa proveedora que procesen o alberguen información responsabilidad de Izenpe estarán sincronizados entre sí y con la hora oficial.

4.8. SEGURIDAD DE SISTEMAS

Todos los servicios que se presten mediante el uso de infraestructura TIC de la empresa proveedora deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad de sistemas:

1. Los sistemas de información que alberguen o traten información responsabilidad de Izenpe deberán registrar los eventos más significativos en torno a su funcionamiento. Estos registros de actividad estarán contemplados dentro de la política de backup de la organización.
2. La empresa proveedora del servicio garantizará que la capacidad de los sistemas de información que guarden o traten información responsabilidad de Izenpe se gestiona



adecuadamente, evitando potenciales paradas o malos funcionamientos de dichos sistemas por saturación de recursos.

3. Los sistemas de información que alberguen o procesen información responsabilidad de Izenpe estarán adecuadamente protegidos frente a software malicioso, aplicando las siguientes precauciones:
 1. Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles, en los entornos de prueba, desarrollo y producción.
 2. El software antivirus se deberá instalar y usar en todos los servidores y ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
 3. El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática, de los ficheros de definición de virus tanto en los ordenadores personales como servidores, así como de bloqueo frente a la detección de virus informáticos.
 4. La empresa proveedora establecerá una política de copias de seguridad que garantice la salvaguarda de cualquier dato o información relevante para el servicio prestado, con una periodicidad máxima mensual.
 5. Siempre que se utilice el correo electrónico en relación al servicio prestado, la empresa proveedora deberá respetar las siguientes premisas:
 - a) No se permitirá la transmisión vía correo electrónico de información confidencial de Izenpe salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
 - b) No se permitirá la transmisión vía correo electrónico de información que contenga datos de carácter personal de nivel alto, salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
 6. Siempre que para la prestación del servicio se haga uso del correo electrónico de Izenpe se deberán respetar, al menos, los siguientes principios:
 - a) Se considerará al correo electrónico como una herramienta más de trabajo proporcionada con el fin exclusivo del servicio contratado. Esta consideración facultará a Izenpe a implementar sistemas de control destinados a velar por la protección y el buen uso de este recurso. Esta facultad, no obstante, se ejercerá salvaguardando la dignidad de las personas y su derecho a la intimidad.
 - b) El sistema de correo electrónico de Izenpe no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.
 - c) Las personas usuarias no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples personas usuarias).
 7. El acceso a los sistemas de información que alberguen o procesen información responsabilidad de Izenpe deberá realizarse siempre de forma autenticada, al menos mediante la utilización de un identificador de persona usuaria unipersonal y una contraseña asociada. Esta obligación deberá ser cumplida tanto por las personas usuarias “normales” como especialmente por las personas usuarias con privilegios de administración de dichos sistemas de información.



8. Los sistemas de información que alberguen o procesen información responsabilidad de Izenpe deberán contar con sistemas de control de acceso que limiten el acceso a dicha información exclusivamente al personal del servicio.
9. Las sesiones de acceso a los sistemas de información que alberguen o procesen información responsabilidad de Izenpe deberán bloquearse automáticamente tras un cierto tiempo de inactividad de las personas usuarias.
10. Siempre que se haga uso de software facilitado por Izenpe se deberán atender las siguientes políticas:
 1. Todo el personal que acceda a los Sistemas de Información debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.
 2. Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.
 3. Está prohibido desinstalar cualquiera de los programas instalados por Izenpe.

4.9. SEGURIDAD DE RED

Todas las empresas proveedoras de servicios que se presten mediante el uso de infraestructura TIC de la empresa proveedora deberán garantizar respecto a la información responsabilidad de Izenpe que se cumplen, al menos, las siguientes políticas de seguridad de red:

- a) Las redes a través de las que circule la información deberán estar adecuadamente gestionadas y controladas, asegurándose de que no existen accesos no controlados ni conexiones cuyos riesgos no estén apropiadamente gestionados por la empresa proveedora.
- b) Los servicios disponibles en las redes a través de las que circule la información deberán limitarse en la medida de lo posible.
- c) Las redes que permitan el acceso a la infraestructura TIC de Izenpe deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:
 1. El acceso de personas usuarias remoto a la red de Izenpe estará sujeto al cumplimiento de procedimientos de autenticación previa y validación del acceso.
 2. Estas conexiones se realizarán por tiempo limitado y mediante la utilización de redes privadas virtuales o líneas dedicadas.
 3. En estas conexiones no se permitirá ningún tipo de equipo de comunicaciones (hubs, switches, etc.) que posibilite conexiones alternativas no controladas.
- d) El acceso a las redes a través de las que circule la información deberá estar limitado.
- e) Todos los equipos conectados a las redes a través de las que circule la información deberán estar apropiadamente identificados, de modo que el tráfico de red pueda ser identificable.
- f) El teletrabajo, considerado como el acceso a la red corporativa desde el exterior, se regula mediante la aplicación de las siguientes políticas:
 - a) Se establecerán criterios de autorización del teletrabajo en base a las necesidades del puesto de trabajo.



- b) Se establecerán las medidas necesarias para la conexión segura a la red corporativa.
- c) Se establecerán sistemas de monitorización y auditoría de seguridad para las conexiones establecidas.
- d) Se controlará la revocación de derechos de acceso y devolución de equipamiento tras la finalización del periodo de necesidad del mismo.

4.10. TRAZABILIDAD DE USO DE LOS SISTEMAS

Todas las empresas proveedoras de servicios que impliquen el acceso a los sistemas de información de Izenpe y que se presten mediante el uso de infraestructura TIC de la empresa proveedora deberán garantizar que se cumplen, al menos, las siguientes políticas de trazabilidad de uso de los sistemas:

1. Se registrarán los accesos privilegiados conservándose dichos registros de acuerdo a la política de copias de seguridad de la organización.
2. Se registra la actividad de los sistemas utilizados para llevar a cabo dicho acceso privilegiado, conservándose dichos registros de acuerdo a la política de copias de seguridad de la organización.
3. Los errores y fallos registrados en la actividad de los sistemas se analizan, adoptándose las medidas necesarias para su subsanación.

4.11. CONTROL Y GESTIÓN DE IDENTIDADES Y ACCESOS

Todos los servicios que se presten mediante el uso de infraestructura TIC de la empresa proveedora deberán garantizar que se cumplen, al menos, las siguientes políticas de control y gestión de identidades y accesos a la hora de acceder a información responsabilidad de Izenpe:

1. Todas las personas usuarias con acceso a un sistema de información dispondrán de una autorización de acceso unipersonal.
2. Las personas usuarias son responsables de toda actividad relacionada con el uso de su acceso autorizado.
3. Las personas usuarias no deben utilizar ningún acceso autorizado de otra persona usuaria, aunque dispongan de la autorización de la persona propietaria.
4. Las personas usuarias no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.
5. Deberá haber una política de seguridad de contraseñas.
6. La empresa proveedora deberá garantizar que periódicamente se constata que sólo tienen acceso a la información responsabilidad de Izenpe el personal debidamente autorizado para ello.
7. En aquellos casos en los que además se acceda a los sistemas de información de Izenpe se deberán considerar, además, las siguientes políticas adicionales:
 - Las personas usuarias tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.



- En caso de que el sistema no lo solicite automáticamente, la persona usuaria debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
- En el caso que el sistema no lo solicite automáticamente, la persona usuaria debe cambiar su contraseña como mínimo una vez cada 90 días. En caso contrario, se le podrá denegar el acceso y deberá contactar con el CAU para la obtención de una nueva.
- Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
- En relación a datos de carácter personal, exclusivamente el personal autorizado para ello podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos, conforme a los criterios establecidos por la persona responsable del fichero.
- Si una persona usuaria tiene sospechas de que su acceso autorizado (identificador de persona usuaria y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y contactar con el CAU para notificar la incidencia.

4.12. GESTIÓN DE CAMBIOS

Todas las empresas proveedoras de servicios que impliquen el acceso a los sistemas de información de Izenpe deberán garantizar que se cumplen, al menos, las siguientes políticas de gestión de cambios:

1. Todos los cambios que se lleven a cabo se deberán realizar siguiendo un procedimiento formalmente establecido y documentado, que garantice que se siguen los pasos apropiados para realizar el cambio.
2. El procedimiento de gestión de cambios deberá garantizar que se minimizan los cambios sobre los componentes críticos, limitándose a los estrictamente imprescindibles.
3. Se deberán verificar todos los cambios sobre los componentes críticos, para comprobar que no se producen efectos adversos colaterales o no previstos sobre el funcionamiento de dichos componentes o sobre su seguridad.
4. Las empresas proveedoras deberán analizar las vulnerabilidades técnicas que presenten las infraestructuras utilizadas para la prestación del servicio, informando a Izenpe de todas aquellas asociadas a los componentes críticos, con el fin de gestionar conjuntamente dichas vulnerabilidades.

4.13. SEGURIDAD EN DESARROLLO

Todas las empresas proveedoras de servicios que impliquen el acceso a los sistemas de información de Izenpe y que realicen actividades de desarrollo de aplicativos deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad en dicha actividad:

1. Todo el proceso de desarrollo de software externalizado será controlado y supervisado por Izenpe y se desarrollará de acuerdo a un proceso formal que determine las reglas a seguir.



2. Se incorporarán mecanismos de identificación, autenticación, control de acceso, auditoría e integridad en todo el ciclo de vida de diseño, desarrollo, implementación y operación de los aplicativos.
3. Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.
4. Las aplicaciones que se desarrollen deberán incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.
5. Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.
6. Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.
7. Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.
8. El acceso al código fuente de los aplicativos deberá estar limitado al personal del servicio.
9. Durante las fases de desarrollo y pruebas se llevarán a cabo pruebas específicas de las funcionalidades de seguridad.
10. En los entornos de pruebas y desarrollo sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.
11. Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.
12. Se establecerá un sistema de control de versiones que permitan la trazabilidad sobre el desarrollo del código.
13. Los entornos con los que se lleven a cabo los desarrollos deberán estar aislados entre sí y también aislados de los entornos de producción en los que se albergue o procese la información.

4.14. GESTIÓN DE CONTINGENCIAS

Todos los servicios que se presten mediante el uso de infraestructura TIC de la empresa proveedora deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad en dicha actividad:

- a) El servicio cuenta con un plan que permite su prestación incluso en caso de contingencias.
- b) El plan anterior ha sido desarrollado en función de los eventos capaces de causar interrupciones en el servicio y su probabilidad de ocurrencia.
- c) La empresa proveedora puede demostrar la viabilidad del plan de contingencias existente.



4.15. FINALIZACIÓN DEL CONTRATO SUSCRITO CON IZENPE

Se deben acordar por contrato con el proveedor las medidas a cumplir tras la conclusión del contrato, incluyendo como mínimo las siguientes medidas de seguridad:

- Destrucción de información.
- Depósito en custodia, retorno y devolución de los activos (hardware de TI, claves criptográficas, software, documentos, informes y medios).
- Revocación del acceso físico y lógico y la conectividad de la red.
- Protección y aseguramiento de la Propiedad Intelectual.
- Traspaso de conocimiento.
- Acuerdos de no competencia.

5. SEGUIMIENTO Y CONTROL

Con el fin de velar por el correcto uso de los recursos, a través de los mecanismos formales y técnicos que se considere oportunos, Izenpe comprobará, ya sea de forma periódica o cuando por razones específicas de seguridad o del servicio resulte conveniente, la correcta utilización de dichos recursos por todas las personas usuarias.

- En caso de apreciar el uso incorrecto de aplicaciones y/o datos, o cualquier otro recurso informático, se comunicará tal circunstancia a la entidad empresa proveedora y se facilitará, en su caso, la formación necesaria para el correcto uso de los recursos.
- En caso de apreciarse mala fe en la utilización de las aplicaciones, datos, así como cualquier otro recurso informático, Izenpe ejercerá las acciones que legalmente le amparen para la protección de sus derechos.

6. ACTUALIZACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Debido a la evolución de la tecnología, las amenazas de seguridad y a los nuevos requerimientos legales, Izenpe se reserva el derecho a modificar esta Política.

Los cambios realizados en estas políticas serán divulgados a todas las entidades proveedoras de servicios a las que les aplique utilizando los medios que se consideren pertinentes. Es responsabilidad de cada entidad proveedora garantizar la lectura y conocimiento de las políticas de seguridad más recientes de Izenpe por parte de su personal.