POLÍTICA DE SEGURIDAD PARA PROVEEDORES

Referencia:	IZENPE-Política Seguridad Proveedores
Nº Versión:	v 1.00
Fecha:	10 de noviembre de 2016

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

www.izenpe.com
info@izenpe.com
Tel.: 945 06 77 23

Histórico de versiones:

VERSIÓN	FECHA	HISTÓRICO DE CAMBIOS
1.0	10/11/2016	Versión inicial

Índice

1. INTRODUCCIÓN

1.1 PROPÓSITO

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

Su finalidad es evitar posibles pérdidas o usos indebidos de información que pueda dañar o perjudicar la reputación de la Sociedad. Para ello esta Política describe qué espera Izenpe del personal que trabaja para esta organización pero que pertenece a otras empresas proveedoras, y que en el desarrollo de sus funciones pudiera tener acceso a información, sistemas de información o recursos de la Sociedad.

Se pretende proteger la confidencialidad, integridad y disponibilidad de la información y sistemas de Izenpe.

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

1.2 ÁMBITO DE APLICACIÓN

Esta Política será de aplicación a todas las actividades desarrolladas por personal que preste servicios para Izenpe pero que pertenece a otras empresas proveedoras, vinculada a través del correspondiente marco contractual.

- El apartado 2 POLÍTICAS *GENERALES DE SEGURIDAD PARA PROVEEDORES*, será aplicable a cualquier proveedor, independientemente del tipo de servicio proporcionado.
- Cada uno de los sub-apartados del apartado *3 POLÍTICAS ESPECÍFICAS DE SEGURIDAD PARA PROVEEDORES* de la presente política será aplicable exclusivamente a aquellos proveedores cuyos servicios proporcionados se correspondan con el tipo de servicio indicado en cada caso, tal y como se indica al comienzo del citado apartado.

2. POLÍTICAS GENERALES DE SEGURIDAD PARA PROVEEDORES

2.1 PRESTACIÓN DE SERVICIOS A IZENPE

1. Las actividades desarrolladas por el personal perteneciente a empresas proveedoras se realizarán de acuerdo a lo establecido en el correspondiente contrato regulador, así como a las normas y procedimientos establecidos a tal efecto entre Izenpe y el proveedor.
2. La empresa proveedora proporcionará a Izenpe periódicamente 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 contrato, todo el personal externo que desarrolle labores para Izenpe deberá cumplir con lo determinado en este documento.

   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 empresa contratada, y que pueden llegar a la resolución de los contratos vigentes.
4. La empresa 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 empresas 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 contrato.
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.

2.2 CONFIDENCIALIDAD DE LA INFORMACIÓN

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 ofimáticas dispuestas por Izenpe y 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 empresa 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 empresa 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.

Para garantizar la seguridad de los datos de carácter personal, el personal que pertenece a empresas proveedoras deberá observar además las siguientes normas de actuación,

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.

2.3 PROPIEDAD INTELECTUAL

1. Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.
2. El personal externo únicamente podrá utilizar material autorizado por Izenpe para el desarrollo de sus funciones.

3. Queda estrictamente prohibido el uso de programas informáticos en los sistemas de información de Izenpe sin la correspondiente licencia.
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.

2.4 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 contrato. 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 toda clase de material pornográfico, mensajes o de una 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 es de alguna u otra manera confidencial.
    d) Transmisión o recepción de ficheros que infrinjan la normativa de protección de datos de carácter personal o directrices de Izenpe.
    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, dicho tratamiento deberá ser autorizado expresamente por la organización y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.
5. La transmisión de datos de carácter personal de nivel alto, a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

2.5 USO APROPIADO DE LOS RECURSOS

1. El proveedor se compromete a informar periódicamente a Izenpe de los activos con los que proporciona el servicio.
2. El proveedor se compromete a utilizar los recursos dispuestos para la provisión del servicio de acuerdo a las condiciones para las que fueron diseñados e implantados.
3. Los recursos que Izenpe pone a disposición del personal externo, (informáticos, datos, software, redes, sistemas de comunicación, etc.), están 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.
4. Todos los equipos del proveedor que se conecten a la red de Izenpe deberán estar homologados. El proveedor pondrá a disposición de Izenpe dichos equipos para que Izenpe instale el software homologado y se configuren adecuadamente.
5. Cualquier fichero introducido en la red 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.
6. Se deberán restituir a Izenpe todos los activos físicos y destruir o restituir a todos los activos de información, sin retraso injustificado, después de la finalización del contrato. Finalizado el servicio Izenpe formateará todos los ordenadores en los que se haya instalado software.
7. 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 de producción de Izenpe de equipos y/o aplicaciones que no estén especificados como parte del Software o de los ¿Estándares de los Recursos Informáticos? propios de Izenpe o bajo su supervisión.
    c) Introducir en los Sistemas de Información o la Red de Izenpe contenidos obscenos, amenazadores, inmorales u ofensivos.
    d) 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.
    e) Intentar acceder sin autorización explícita a áreas restringidas de los Sistemas de Información de Izenpe.
    f) Intentar distorsionar o falsear los registros “log” de los Sistemas de Información de Izenpe.

g) 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.

h) Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos de Izenpe.

i) Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos responsabilidad de Izenpe.

2.6 RESPONSABILIDADES DEL USUARIO

1. Los proveedores de servicios deberán asegurarse 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 usuario y todo lo que de él se derive. Por lo tanto, es imprescindible que cada persona mantenga bajo control los sistemas de autenticación asociados a su identificador de usuario, garantizando que la clave asociada sea únicamente conocida por el propio usuario, no debiendo revelarse al resto del personal bajo ningún concepto.

    b) Los usuarios no deberán utilizar ningún identificador de otro usuario aunque dispongan de la autorización del propietario.

    c) Los usuarios 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 con acceso 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 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 scanner y fax) como los equipos de duplicado (fotocopiadora, fax y scanner). La reproducción o envío de información con este tipo de dispositivos quedará bajo la responsabilidad del usuario.
    c) Retirar, sin retraso injustificado, cualquier información confidencial, 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, en caso de identificarse incidentes o debilidades que puedan suponerse relacionadas con la seguridad de la información.
    g) Ninguna persona intentará sin autorización explícita ni por ningún medio, transgredir el sistema de seguridad y las autorizaciones. Se prohíbe la captura de tráficos de red por parte de los usuarios, salvo que se estén llevando a cabo tareas de auditoría expresamente autorizadas.
    h) Ningún dato de carácter personal será almacenado en equipos de usuario ni soportes de información.
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) Proteger todos los sistemas de información y redes de telecomunicaciones contra accesos o usos no autorizados, interrupciones de operaciones, destrucción, mal uso o robo.
    c) Contar con la autorización necesaria para obtener el acceso a los sistemas de información y/o la información accedidos.
    d) Conocer, aceptar y cumplir esta Política antes de acceder a la información y/o los sistemas de Izenpe.

2.7 EQUIPOS DE USUARIO

1. Los proveedores de servicios deberán asegurarse de que todo el equipamiento informático de usuario utilizado para acceder a información responsabilidad de Izenpe cumple las siguientes políticas:

    a) Cuando se desatienda un puesto durante un periodo corto de tiempo el sistema deberá activar su bloqueo.

    b) Ningún equipo de usuario dispondrá de herramientas que puedan transgredir el sistema de seguridad y las autorizaciones dentro de los sistemas de la organización.

    c) Los equipos de usuario se mantendrán de acuerdo a las especificaciones del fabricante.

    d) Todos los equipos de usuario están adecuadamente protegidos frente a malware:

    - El software antivirus se deberá instalar y usar en todos los ordenadores personales para reducir el riesgo operacional asociado con los virus u otro software malicioso.
    - Se mantendrán al día con las últimas actualizaciones de seguridad disponibles. El software antivirus deberá estar siempre habilitado. Se establecerá una actualización automática de los ficheros de definición de virus.

2. Se velará especialmente por la seguridad de todos los equipos móviles de usuario 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 Izenpe para evitar la visión accidental por parte de terceras personas.

2.8 GESTIÓN DE EQUIPAMIENTO “HARDWARE”

Los proveedores de servicios deberán asegurarse de que todos los equipos proporcionados por Izenpe para la prestación de servicios, independientemente del tipo que sean, se gestionan apropiadamente. Para ello deberán cumplir las siguientes políticas:

1) El proveedor deberá mantener una relación actualizada de equipos y usuarios de dichos activos, o responsables asociados en caso de que los activos no sean de uso unipersonal

   Dicha relación podrá ser requerida por Izenpe en cualquier momento.

2) Siempre que un proveedor quiera reasignar algún equipo de Izenpe que haya contenido información responsabilidad de Izenpe deberá devolver temporalmente dicho activo para que se puedan llevar a cabo los procedimientos de borrado seguro necesarios de forma previa a su reasignación.

3) En caso de que un proveedor quiera proceder a dar de baja algún deberá devolver a Izenpe dicho activo, para que se pueda tratar dicha baja de forma apropiada.

4) En caso de que un proveedor cese en la prestación del servicio, deberá devolver toda la relación de equipos recibidos, tal y como establecen los correspondientes contratos de prestación de servicios. Sólo en el caso de ¿activos de información? el proveedor podrá proceder a su eliminación segura, en cuyo caso deberá notificar a Izenpe dicha eliminación.

3. POLÍTICAS ESPECÍFICAS DE SEGURIDAD PARA PROVEEDORES

3.1 APLICABILIDAD DE LAS POLÍTICAS ESPECÍFICAS DE SEGURIDAD PARA PROVEEDORES

Todos los proveedores deberán cumplir, además de las políticas generales de seguridad para proveedores, las políticas específicas de seguridad recogidas en el presente apartado que les correspondan en cada caso, en función de las características del servicio prestado.

Las tipologías de servicio que se contemplan son las que se indican a continuación.

a) **Lugar de ejecución del servicio.**

En función del lugar principal en el que se desarrollen los servicios se distinguen dos casos:

- Izenpe: El proveedor presta el servicio principalmente en las dependencias de Izenpe.
- Remoto: El proveedor presta el servicio principalmente desde sus propias dependencias, pese a que se puedan llevar a cabo actividades puntuales en las dependencias de Izenpe.

b) **Nivel de acceso** a los sistemas de Izenpe.

En función del nivel de acceso a los sistemas de información se distinguen dos casos:

- Con acceso de nivel de usuario: 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 usuario que les permiten acceder a alguno de dichos sistemas con privilegios habituales.
- Con acceso privilegiado: El servicio prestado requiere de la capacidad de acceso privilegiado a los sistemas de información de Izenpe, con capacidad para administrar dichos sistemas y/o los datos de producción que procesan.

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

	Lugar		Nivel de acceso	
	Izenpe	Remoto	Privilegiado	Normal
Selección de personal			X	
Auditoría de seguridad			X	
Comunicación de incidencias	X	X	X	X
Seguridad física		X		
Gestión de activos		X		
Arquitectura de seguridad		X	X	X
Seguridad de sistemas		X		
Seguridad de red		X		
Trazabilidad de uso de los sistemas		X	X	
Control y gestión de identidades y accesos		X		
Gestión cambios	X	X	X	X
Seguridad en desarrollo			X	X
Gestión contingencias		X		

3.2 SELECCIÓN DE PERSONAL

Los proveedores de Izenpe que requieran acceder a los sistemas de información de Izenpe deberán cumplir las siguientes políticas de selección de personal:

1. Deberá 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,.

3.3 AUDITORÍA DE SEGURIDAD

Todos los proveedores de servicios que requieran acceder a los sistemas de información de Izenpe deberán cumplir las siguientes políticas de auditoría de seguridad:

1. El proveedor 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 el proveedor del servicio.
3. Izenpe se reserva el derecho de realizar auditorías extraordinarias adicionales, siempre que se den causas específicas que lo justifiquen.

3.4 COMUNICACIÓN DE INCIDENCIAS

Todos los proveedores de servicios que accedan (tanto privilegiado como no privilegiado) a los sistemas de información de Izenpe independientemente del lugar desde el que se preste el servicio deberán cumplir las siguientes políticas de comunicación de incidencias:

1. Todo el personal asignado al servicio deberá ponerse en contacto con el Responsable de Seguridad de Izenpe en caso de que detecte cualquier incidencia relacionada con la información o los recursos de Izenpe.
2. Cualquier usuario podrá trasladar al 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 Responsable de Seguridad de Izenpe cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos, etc.
4. El Responsable de Seguridad de Izenpe centraliza la recogida, análisis y gestión de las incidencias recibidas.
5. Si no estuviera disponible el Responsable de Seguridad de Izenpe se deberán comunicar al Responsable del Área Técnica de Izenpe.

3.5 SEGURIDAD FÍSICA

Todos los proveedores que presten los servicios desde la sede del proveedor deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad física:

1. 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.
2. Existirá algún tipo de control de las visitas, al menos en áreas de acceso público y/o de carga y descarga.
3. 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.
4. 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:
    a) El área especialmente protegida deberá tener un sistema de control de acceso independiente al de la sede.
    b) 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.
    c) Se mantendrá un registro de todos los accesos de personas ajenas.
    d) El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.

e) El consumo de alimentos o bebidas en estas áreas especialmente protegidas estará prohibido.

f) Los sistemas ubicados en estas áreas deberán contar con algún tipo de protección frente a fallos de alimentación.

3.6 GESTIÓN DE ACTIVOS

Todos los proveedores 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 un 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. Se deberá notificar a Izenpe las bajas de los activos utilizados para la prestación del servicio. Si dicho activo contiene otros propiedad de Izenpe (hardware, software u otro tipo de activos), deberá ser entregado a Izenpe previamente a llevar a cabo la baja para que Izenpe proceda a la retirada de los activos de su propiedad.
4. Siempre que un activo haya contenido información responsabilidad de Izenpe, el proveedor 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.

3.7 ARQUITECTURA DE SEGURIDAD

Todos los proveedores de servicios que accedan (tanto privilegiado como no privilegiado) a los sistemas de información de Izenpe y que presten el servicio mediante el uso de infraestructura TIC del proveedor, deberán garantizar que se cumplen, al menos, los siguientes requisitos de arquitectura de seguridad:

1. Siempre que el proveedor de servicios realice trabajos de desarrollo y/o pruebas de aplicaciones para Izenpe o con datos responsabilidad de Izenpe, los entornos con los que se lleven a cabo dichas actividades deberán estar aislados entre sí y también aislados de los entornos de producción en los que se albergue o procese la información.
2. Todos los accesos a los sistemas de información que alberguen o procesen información responsabilidad de Izenpe deberán estar protegidos, al menos, por un cortafuegos que limite la capacidad de conexión a ellos.
3. Los sistemas de información que alberguen o procesen información responsabilidad de Izenpe especialmente sensible deberán estar aislados del resto.
4. Los sistemas de información utilizados para la prestación de servicios deberán contar con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

3.8 SEGURIDAD DE SISTEMAS

Todos los servicios que se presten mediante el uso de infraestructura TIC del proveedor 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. Los relojes de los sistemas del proveedor que procesen o alberguen información responsabilidad de Izenpe estarán sincronizados entre sí y con la hora oficial.
3. El proveedor 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.
4. Los sistemas de información que alberguen o procesen información responsabilidad de Izenpe estarán adecuadamente protegidos frente a software malicioso, aplicando las siguientes precauciones:
    a) Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles, en los entornos de prueba, desarrollo y producción.
    b) 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.
    c) 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.
5. El proveedor 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.
6. Siempre que se utilice el correo electrónico en relación al servicio prestado, el proveedor 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.
7. 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) Los usuarios no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples usuarios).

8. 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 usuario unipersonal y una contraseña asociada. Esta obligación deberá ser cumplida tanto por los usuarios "normales" como especialmente por los usuarios con privilegios de administración de dichos sistemas de información.
9. 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.
10. 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 los usuarios.
11. Siempre que se haga uso de software facilitado por Izenpe se deberán atender las siguientes políticas:

    a) Todo el personal que acceda a los Sistemas de Información debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.

    b) Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

    c) Se prohíbe el uso de software no validado por Izenpe.

    d) También está prohibido desinstalar cualquiera de los programas instalados por Izenpe.

3.9 SEGURIDAD DE RED

Todos los proveedores de servicios que se presten mediante el uso de infraestructura TIC del proveedor deberán garantizar respecto a la información responsabilidad de Izenpe que se cumplen, al menos, las siguientes políticas de seguridad de red:

1. 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 el proveedor.
2. Los servicios disponibles en las redes a través de las que circule la información deberán limitarse en la medida de lo posible.
3. Las redes que permitan el acceso a la infraestructura TIC de Izenpe deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:

a) El acceso de usuarios remotos a la red de Izenpe estará sujeto al cumplimiento de procedimientos de autenticación previa y validación del acceso.

b) Estas conexiones se realizarán por tiempo limitado y mediante la utilización de redes privadas virtuales o líneas dedicadas.

c) En estas conexiones no se permitirá ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas.

4. El acceso a las redes a través de las que circule la información deberá estar limitado.
5. 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.
6. El teletrabajo, considerado como el acceso a la red corporativa desde el exterior, se regula mediante la aplicación de las siguientes políticas:

    1) No se permite la utilización de equipamiento no controlado por Izenpe para las actividades de teletrabajo.

    2) Se establecerán criterios de autorización del teletrabajo en base a las necesidades del puesto de trabajo.

    3) Se establecerán las medidas necesarias para la conexión segura a la red corporativa.

    4) Se establecerán sistemas de monitorización y auditoría de seguridad para las conexiones establecidas.

    5) Se controlará la revocación de derechos de acceso y devolución de equipamiento tras la finalización del periodo de necesidad del mismo.

Siempre que se haga uso del acceso a Internet proporcionado por Izenpe se deberán respetar, adicionalmente, las siguientes políticas:

7. Internet es una herramienta de trabajo. Todas las actividades en Internet deberán estar en relación con tareas y actividades de trabajo. Los usuarios no deben buscar o visitar sitios que no sirvan como soporte al objetivo de negocio de Izenpe o al cumplimiento de su trabajo diario.
8. El acceso a Internet desde la red corporativa se restringe por medio de dispositivos de control incorporado en la misma. La utilización de otros medios de conexión deberá ser previamente validada y estará sujeta a las anteriores consideraciones sobre el uso de Internet.
9. Los usuarios no deberán usar el nombre, símbolo, logotipo o símbolos similares al de IZENPE en ningún elemento de Internet (correo electrónico, páginas web, etc.) no justificado por actividades estrictamente laborales.
10. Únicamente se permitirá la transferencia de datos de o hacia Internet cuando estén relacionadas con actividades del negocio. La transferencia de ficheros no relativa a estas actividades (por ejemplo la descarga de juegos de ordenador, ficheros de sonido y contenidos multimedia, etc.) estarán prohibidas.

3.10 TRAZABILIDAD DE USO DE LOS SISTEMAS

Todos los proveedores de servicios que impliquen el acceso privilegiado a los sistemas de información de Izenpe y que se presten mediante el uso de infraestructura TIC del proveedor 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.

3.11 CONTROL Y GESTIÓN DE IDENTIDADES Y ACCESOS

Todos los servicios que se presten mediante el uso de infraestructura TIC del proveedor 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. Todos los usuarios con acceso a un sistema de información, dispondrán de una autorización de acceso unipersonal compuesta de identificador de usuario y contraseña. Esta obligación deberá ser cumplida tanto por los usuarios “normales” como especialmente por los usuarios con privilegios de administración de dichos sistemas de información.
2. Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
3. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
4. Los usuarios 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. La longitud mínima de la contraseña deberá ser de 6 caracteres.
6. Las contraseñas estarán constituidas por combinación de caracteres alfabéticos y numéricos.
7. Es recomendable utilizar las siguientes directrices para la selección de contraseñas:
    a) No usar palabras conocidas, ni palabras que se puedan asociar con uno mismo, por ejemplo el nombre.
    b) La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos, etc.

c) La clave debería ser algo prácticamente imposible de adivinar. Pero al mismo tiempo debería ser fácilmente recordada por el usuario. Un buen ejemplo es usar el acrónimo de alguna frase o expresión.

d) La clave debería contener al menos un carácter numérico y uno alfabético.

e) La clave no debería empezar ni acabar con un carácter numérico.

f) No se debería utilizar el identificador de usuario como parte de la clave secreta.

8. El proveedor deberá garantizar que periódicamente se constata que sólo tienen acceso a la información responsabilidad de Izenpe el personal debidamente autorizado para ello.

En aquellos casos en los que además se acceda a los sistemas de información de Izenpe se deberán considerar, además, las siguientes políticas adicionales:

9. Ningún usuario recibirá un identificador de acceso a los sistemas de Izenpe hasta que no acepte formalmente la Política de Seguridad vigente.
10. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
11. En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema.
12. En el caso que el sistema no lo solicite automáticamente, el usuario 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 Centro de Atención a Usuarios para la obtención de una nueva.
13. Los accesos autorizados temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.
14. 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 el responsable del fichero.
15. Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña y contactar con el Centro de Atención a Usuarios para notificar la incidencia.

3.12 GESTIÓN DE CAMBIOS

Todos los proveedores 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. Los proveedores 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.

3.13 SEGURIDAD EN DESARROLLO

Todos los proveedores de servicios que impliquen el acceso (tanto privilegiado como no privilegiado) 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, autentificación, 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 el entorno de pruebas 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. Sólo se transferirán al entorno de producción aquellos aplicativos que hayan sido expresamente aprobados.

3.14 GESTIÓN DE CONTINGENCIAS

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

1. El servicio cuenta con un plan que permite su prestación incluso en caso de contingencias.
2. El plan anterior ha sido desarrollado en función de los eventos capaces de causar interrupciones en el servicio y su probabilidad de ocurrencia.
3. El proveedor puede demostrar la viabilidad del plan de contingencias existente.

4. 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 todos los usuarios.

a) En caso de apreciar el uso incorrecto de aplicaciones y/o datos, o cualquier otro recurso informático, se comunicará tal circunstancia a la empresa proveedora y se facilitará, en su caso, la formación necesaria para el correcto uso de los recursos.

b) 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.

5. 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 empresas proveedoras de servicios a las que les aplique utilizando los medios que se consideren pertinentes. Es responsabilidad de cada empresa proveedora garantizar la lectura y conocimiento de las políticas de seguridad más recientes de Izenpe por parte de su personal.