Política de seguridad de la información para proveedores

Versiones de este documento

Versión	Fecha	Descripción	Aprobación
2	04/2025	Ampliación de los principios específicos de seguridad.	Responsable de Seguridad
1	08/2023	Primera Emisión	Responsable de Seguridad

Contenido

Versiones de este documento 2
1 Objeto 4
2 Alcance 4
3 Actualización de las políticas de seguridad 5
4 Principios generales de seguridad 5
4.1 Confidencialidad de la información 6
4.2 Propiedad intelectual 6
4.3 Intercambio de información 7
4.4 Uso apropiado de los recursos corporativos 7
4.5 Responsabilidades del usuario 8
4.6 Equipos de usuario 10
4.7 Gestión de equipamiento Hardware 11
4.8 Supervisión y revisión de los servicios prestados por terceros 11
4.9 Gestión de cambios en la provisión del servicio y cadena de suministro 12
4.10 Comunicaciones 12
4.11 Finalización del contrato 13
5 Principios específicos de seguridad 14
5.1 Aplicabilidad de las políticas específicas de seguridad para Proveedores 14
5.2 Seguridad física 15
5.3 Auditoría de seguridad 16
5.4 Gestión de activos 16
5.5 Arquitectura de seguridad 17
5.6 Seguridad de sistemas 17
5.7 Seguridad de red 19
5.8 Trazabilidad de los sistemas 20
5.9 Control y gestión de identidades y accesos 20
5.10 Gestión de cambios 21
5.11 Seguridad en el desarrollo 22
5.12 Gestión de contingencias 23
5.13 Jurisdicción de los datos 23
5.14 Cifrado y protección de datos 23

1 Objeto

En toda organización existe información cuya pérdida o uso indebido puede dañar su reputación. Asimismo, el deterioro o indisponibilidad de los Sistemas de Información puede interrumpir el normal desarrollo de la operativa, produciendo efectos negativos en la calidad del servicio y los beneficios de la organización.

El principal objetivo de este documento es establecer el marco normativo en relación a la seguridad de la información para los Proveedores de Inerza S.A. (en adelante, INERZA), describiendo lo que se espera de todo el personal que trabaja para INERZA pero que pertenece a otras empresas proveedoras, y que en el desarrollo de sus funciones pueda tener acceso a la información, sistemas de información o recursos de INERZA en general, con el fin de proteger la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información y sistemas manejados por INERZA.

Para ello, las empresas proveedoras a las que se les remitan estas políticas de seguridad se responsabilizan de informar de ellas a las personas que destinen en INERZA, así como de obtener su compromiso por escrito de que se comprometen a respetar dichas Políticas.

La Política de Seguridad refleja requerimientos legales y éticos, tanto en actuaciones informales de los empleados que trabajan para INERZA pertenecientes a empresas proveedoras, como en la realización de su operativa.

Con dicho propósito, esta política contempla lo establecido en las Políticas de Seguridad de INERZA, y refleja las obligaciones a las que está sujeta INERZA por la legislación vigente, y en particular por el reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

2 Alcance

Todas las actividades desarrolladas para INERZA por personal que presta servicios para esta organización pero que pertenece a otras empresas proveedoras (Incluidas las empresas proveedores de servicios en la nube), vinculadas a través del correspondiente contrato de provisión de servicios.

El apartado "*Políticas Generales de Seguridad para Proveedores*" de la presente política será aplicable a cualquier proveedor, independientemente del tipo de servicio proporcionado.

Cada uno de los subapartados del apartado "*Políticas Específicas de Seguridad para Proveedores*" de la presente política será aplicable exclusivamente a aquellos Proveedores cuyos servicios proporcionados se correspondan con la naturaleza del servicio indicado en cada caso, tal y como se indica al comienzo de cada apartado.

3 Actualización de las políticas de seguridad

Debido a la propia evolución de la tecnología, las amenazas de seguridad y a las nuevas aportaciones legales en la materia, INERZA se reserva el derecho a modificar estas políticas cuando sea necesario. 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 INERZA por parte de su personal.

4 Principios generales de seguridad

Los Proveedores sólo podrán desarrollar para INERZA aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios. De este modo, se entenderá que todas las actividades desarrolladas para INERZA por personal perteneciente a empresas proveedoras se encuadran en los contratos de provisión de servicios que vinculan a INERZA con estos Proveedores.

Las actividades desarrolladas por el personal perteneciente a empresas proveedoras se realizarán de acuerdo a lo establecido en el correspondiente contrato de provisión de servicios, así como a las normas y procedimientos establecidos a tal efecto entre INERZA y el Proveedor correspondiente.

Los Proveedores proporcionarán a INERZA, cuando así lo requiera, la relación de personas, perfiles, funciones y responsabilidades asociados al servicio prestado, e informará a través del punto de contacto (POC) de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.

Los Proveedores deberán asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio provisto, tanto a nivel específico en las materias correspondientes a la actividad asociada a la prestación del servicio, como en materia de seguridad de la información, para lo cual deberá asegurarse, al menos, de que todo el personal asociado al servicio conoce y se compromete a cumplir las presentes Políticas de Seguridad.

Todo el personal externo que desarrolle labores de INERZA deberá cumplir con las políticas de seguridad recogidas en el presente documento. En caso de incumplimiento de cualquiera de estas obligaciones, INERZA se reserva el derecho de veto sobre el personal que haya cometido el incumplimiento.

Como mínimo, los Proveedores deberán asegurarse que todo el personal asociado al servicio conoce y se compromete a cumplir lo recogido en esta Política, pudiendo INERZA solicitar en cualquier momento evidencias del proceso de información.

Los Proveedores deberán permitir que INERZA lleve a cabo las auditorías de seguridad que pudiera solicitar, colaborando con el equipo auditor y facilitando todas las evidencias y registros que les sean requeridos.

El alcance de cada auditoría será establecido expresamente por INERZA en cada caso. Las auditorías se llevarán a cabo siguiendo la planificación que se acuerde con el proveedor del servicio.

4.1 Confidencialidad de la información

Toda información, documentación, programas y/o aplicaciones, métodos, organización, estrategias de negocio y actividades relacionadas con INERZA o con su negocio, a las que tenga acceso los Proveedores con objeto de realización del servicio serán considerados información confidencial, en función de lo cual, el acceso, intercambio y tratamiento de dicha información, se realizará siempre de acuerdo a las finalidades previstas descritas en el contrato de prestación de servicios y manteniendo el correspondiente deber de secreto durante la duración del servicio y por tiempo indefinido después de que finalice la relación con INERZA.

Todos los recursos e información a la que haya podido tener acceso o que haya sido necesaria elaborar, modificar o copiar para el correcto desempeño del servicio serán devueltos a la finalización de este. INERZA podrá solicitar el borrado seguro de los dispositivos que hayan tenido acceso a la Información de INERZA.

Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para INERZA.

El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en el artículo 197 el Código Penal, que puede dar derecho a exigir compensaciones.

4.2 Propiedad intelectual

Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por la normativa de propiedad intelectual.

Los Proveedores únicamente podrán utilizar material autorizado por INERZA para el desarrollo de sus funciones.

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

Asimismo, queda prohibido el uso, reproducción, distribución, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual sin la debida autorización por escrito.

INERZA únicamente autorizará el uso de material producido por él mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

4.3 Intercambio de información

Cualquier tipo de intercambio de información que se produzca entre INERZA y los Proveedores se entenderá que ha sido realizado dentro del marco establecido por el contrato de prestación de servicios correspondiente, de modo que dicha información no podrá ser utilizada fuera de dicho marco ni para otros fines.

La distribución de información ya sea en formato electrónico o físico se realizará mediante los recursos determinados en el contrato de prestación de servicios para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato. INERZA se reserva, en función del riesgo identificado, la implantación de medidas de control, registro y auditoría sobre estos recursos de difusión.

En relación con el intercambio de información dentro del marco del contrato de prestación de servicios, se considerarán no autorizadas las siguientes actividades:

- Transmisión o recepción de material protegido por los derechos de autor infringiendo la Ley de Protección Intelectual.
- Transmisión o recepción de toda clase de material pornográfico, de naturaleza sexual explícita, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.
- Transmisión o recepción de información sensible (por ejemplo, datos relativos a la salud de las personas), salvo que la comunicación electrónica esté cifrada y el envío esté autorizado por escrito.
- Transferencia de información protegida a terceras partes no autorizadas.
- Transmisión o recepción de aplicaciones no relacionadas con el negocio.
- Participación en actividades de Internet, como grupos de noticias, juegos u otras que no estén directamente relacionadas con la prestación del servicio.
- Todas las actividades que puedan dañar la imagen y reputación de INERZA están prohibidas en Internet y en cualquier otro lugar.

4.4 Uso apropiado de los recursos corporativos

Los Proveedores se comprometen a utilizar los recursos dispuestos para la provisión del servicio de acuerdo con las condiciones para las que fueron diseñados e implantados.

Los recursos que INERZA pone a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplimentar las obligaciones y propósito de la operativa para la que fueron proporcionados. INERZA se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

Cualquier fichero introducido en la red de INERZA 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 software malicioso.

Se deberán restituir a INERZA todos los activos físicos y destruir o restituir a INERZA todos los activos de información, sin retraso injustificado, después de la finalización del contrato.

Se prohíbe expresamente:

- El uso de los recursos proporcionados por INERZA para actividades no relacionadas con el propósito del servicio.
- Introducir en los Sistemas de Información o la Red de INERZA contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente en la red de INERZA 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. Todo el personal con acceso a la red de INERZA tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Intentar obtener sin autorización expresa otros derechos o accesos distintos a aquellos que INERZA les haya asignado.
- Intentar acceder sin autorización expresa a áreas restringidas de los Sistemas de Información de INERZA.
- Intentar distorsionar o falsear los registros “log” de los Sistemas de Información de INERZA.
- Intentar descifrar sin autorización expresa las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de INERZA.
- Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros Usuarios, ni dañar o alterar los Recursos Informáticos de INERZA.
- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos responsabilidad de INERZA (Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal).
- Albergar Datos de Carácter Personal de INERZA o cuyo tratamiento haya sido encargado a INERZA en las unidades locales de disco de los puestos de usuario.

4.5 Responsabilidades del usuario

Los Proveedores deberán asegurarse de que todo el personal que en el desarrollo de sus funciones para INERZA pueda tener acceso a la información, sistemas de información o recursos de INERZA respete los siguientes principios básicos dentro de su actividad:

- Cada persona con acceso a información de INERZA 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.
- Los usuarios no deberán utilizar ningún identificador de otro usuario, aunque dispongan de la autorización del propietario.
- Los usuarios conocen y aplican los requisitos y procedimientos existentes en torno a la información manejada.
- Cualquier usuario con acceso a información de INERZA deberá seleccionar contraseñas acordes a la política de contraseñas de INERZA:
  - Seleccionar contraseñas de calidad.
  - Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
  - Cambiar las contraseñas periódicamente y evitar reutilizar o reciclar viejas contraseñas.
  - Cambiar las contraseñas por defecto y las temporales en el primer inicio de sesión (“login”).
  - Evitar el uso de utilidades tipo “recordar contraseña”.
- Cualquier usuario con acceso a información de INERZA deberá velar por que los equipos queden protegidos cuando vayan a quedar desatendidos.
- Cualquier usuario con acceso a información responsabilidad de INERZA deberá respetar al menos las siguientes 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:
  - Almacenar bajo llave los documentos en papel y los medios informáticos con información responsabilidad de INERZA en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
  - No dejar desatendidos los equipos asignados a funciones críticas de INERZA, y bloquear su acceso cuando sea estrictamente necesario.
  - Proteger, siempre que se utilice información responsabilidad de INERZA, tanto los puntos de recepción y envío de información (correo postal, máquinas de scanner) como los equipos de duplicado (fotocopiadora, scanner). La reproducción o envío de información con este tipo de dispositivos quedará bajo la responsabilidad del usuario.
  - Retirar, sin retraso injustificado, cualquier información confidencial que sea responsabilidad de INERZA, una vez impresa.
  - Los listados con datos de carácter personal o información confidencial responsabilidad de INERZA deberán almacenarse en lugar seguro al que únicamente tengan acceso personal autorizado.

- Los listados con datos de carácter personal o información confidencial responsabilidad de INERZA deberán eliminarse de manera segura una vez no sean necesarios.
- Los usuarios con acceso a sistemas y/o información de INERZA nunca deberán sin autorización expresa y por escrito, 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.
- Ningún usuario con acceso a sistemas y/o información de INERZA intentará sin autorización expresa y por escrito por ningún medio vulnerar 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 o sea necesario para resolver alguna incidencia.
- Ningún dato de carácter personal responsabilidad de INERZA será almacenado en equipos de usuario ni en soportes de información.

4.6 Equipos de usuario

Los Proveedores de servicios deberán asegurarse de que todo el equipamiento informático de usuario utilizado para acceder a información responsabilidad de INERZA cumple las siguientes políticas:

- Cuando se desatiende un puesto durante un periodo corto de tiempo el sistema deberá activar su bloqueo.
- Ningún equipo de usuario dispondrá de herramientas que puedan vulnerar el sistema de seguridad y las autorizaciones dentro de los sistemas de la organización salvo que sea necesario para la provisión del servicio.
- Los equipos de usuario se mantienen de acuerdo a las especificaciones del fabricante.
- 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.
- Se velará especialmente por la seguridad de todos los equipos móviles de usuario que contengan información responsabilidad de INERZA o permitan acceder a ella de algún modo:
  - Verificando que no incluyen más información responsabilidad de INERZA que la que sea estrictamente necesaria.
  - Garantizando que se aplican controles de acceso a dicha información.

- Minimizando los accesos a dicha información en presencia de personas ajenas al servicio provisto a INERZA.
- Transportando los equipos en fundas, maletines o equipamiento similar que incorpore la apropiada protección frente a golpes.
- Tomando especiales precauciones en el exterior de las dependencias de INERZA para evitar la visión accidental por parte de terceras personas de la información responsabilidad de INERZA.

4.7 Gestión de equipamiento Hardware

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

- Los Proveedores deberán 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 INERZA en cualquier momento.
- Siempre que los Proveedores quieran reasignar algún equipo que haya contenido información responsabilidad de INERZA, llevarán a cabo los procedimientos de borrado seguro necesarios de forma previa a su reasignación.
- En caso de que los Proveedores cesen en la prestación del servicio, deberán devolver a INERZA toda la relación de equipos recibidos. Sólo en el caso de activos de información el proveedor podrá proceder a su eliminación segura, en cuyo caso deberá notificar a INERZA dicha eliminación.

4.8 Supervisión y revisión de los servicios prestados por terceros

Todos los Proveedores quedan obligados a facilitar las métricas necesarias que permitan a INERZA verificar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) acordados entre ambas partes.

Dichas métricas podrán ponerse a disposición de INERZA de cualquiera de las siguientes formas:

- Facilitando el acceso a una plataforma web o similar donde INERZA pueda supervisar y auditar los niveles de servicio recibido.
- Remitiendo mensualmente la información sobre los niveles de servicio al punto de contacto (POC).

INERZA se reserva el derecho de realizar un seguimiento de los servicios contratados al objeto de verificar el cumplimiento de los acuerdos firmados y a rescindir el contrato en caso de incumplimiento reiterado.

Todos los Proveedores comunicarán a INERZA el procedimiento de incidencias y escalado y facilitarán un punto de contacto (e-mail) donde poder recibir las comunicaciones de INERZA.

4.9 Gestión de cambios en la provisión del servicio y cadena de suministro

Los Proveedores deberán informar por escrito a través del punto de contacto (POC) a INERZA:

- Cualquier cambio que afecte a la provisión del servicio, incluyendo, entro otros, el mantenimiento y la mejora de las políticas, los procedimientos y controles de seguridad de la información.
- Cualquier subcontratación total o parcial del servicio prestado con la antelación suficiente para su estudio por parte de INERZA, pudiéndose solicitar medidas de seguridad adicionales o rechazarse la subcontratación. En el supuesto de que INERZA lo autorice por escrito, la empresa subcontratista o cesionaria debidamente autorizada, quedará subrogada a todas las obligaciones y derechos de la subcontratista principal, en lo que se refiere a la parte del contrato cedido o subrogada y, por lo tanto, deberá cumplir con la presente Política de Seguridad para empresas proveedoras de INERZA.

Los Proveedores se comprometen a exigir y extender a su cadena de suministro los requisitos de seguridad en la medida necesaria y de acuerdo con los resultados del correspondiente análisis de riesgos.

4.10 Comunicaciones

4.10.1 Punto de contacto (POC)

El punto de contacto con INERZA, en caso de no especificarse ningún otro en el contrato, será la siguiente dirección de email: facturacion@inerza.com.

4.10.2 Incidentes de seguridad

Los Proveedores se comprometen a comunicar de manera inmediata cualquier incidente, debilidad o amenaza (observada o sospechada) que detecte en los sistemas de información de INERZA o que haya podido afectar a información propiedad de INERZA o de sus clientes, a través del envío de un e-mail a: servicedesk@inerza.com.

Este compromiso aplica igualmente al personal desplazado en las instalaciones de INERZA.

4.10.3 Mantenimiento

Toda actuación de mantenimiento que se vaya a realizar tanto en los sistemas de información como en las instalaciones físicas de INERZA deberá ser comunicada con 3 días hábiles de antelación al punto de contacto (POC).

4.11 Finalización del contrato

A la finalización del contrato los Proveedores deberán ejecutar un plan para transferir el servicio de forma ordenada. Esto implica presentar una planificación detallada que incluya los medios a utilizar, acciones de contingencia y riesgos del proceso, considerando además un período de transición si es necesaria la incorporación de un nuevo Proveedor.

5 Principios específicos de seguridad

5.1 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 según les corresponda en cada caso, en función del servicio prestado.

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

- **Lugar de ejecución del servicio:** en función del lugar principal en el que se desarrollen los servicios se distinguen 2 casos:
  - **INERZA:** El proveedor presta el servicio principalmente desde las propias instalaciones de INERZA.
  - **REMOTO:** El proveedor presta el servicio principalmente desde sus propias instalaciones, pese a que se puedan llevar a cabo actividades puntuales en las instalaciones de INERZA.
- **Nivel de acceso** a los sistemas de INERZA: El servicio prestado requiere de la utilización de sistemas de información de INERZA, para lo cual se requieren cuentas de usuario (con nivel de acceso privilegiado o no).
- **Propiedad de la infraestructura TIC** utilizadas: en función de quien sea el propietario de las principales infraestructuras TIC (comunicaciones, equipos de usuario, software, etc) utilizadas para prestar el servicio se distinguen 2 casos:
  - **INERZA:** La mayor parte de las infraestructuras TIC utilizadas para presta el servicio son propiedad de INERZA, siendo las proporcionadas por el proveedor una minoría o complementarias.
  - **PROVEEDOR:** La mayor parte de las infraestructuras TIC utilizadas para prestar el servicio con propiedad del Proveedor, siendo poco significativas las proporcionadas por INERZA.

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		ACCESO	INFRAESTRUCTURA TIC	
	Instalaciones CTSA	Instalaciones Proveedor	Normal / privilegiado	Infraestructura CTSA	Infraestructura Proveedor
Seguridad física		x			
Auditoría de seguridad			x	x	x
Gestión de activos				x	x
Arquitectura de seguridad		x	x		x
Seguridad de sistemas					x
Seguridad de la red		x	x		x
Trazabilidad de los sistemas			x		x
Control y gestión de identidades y accesos			x		
Gestión de cambios					x
Seguridad en el desarrollo				x[1]	x[1]
Gestión de contingencias		x			x
Jurisdicción de los datos					x[2]
Cifrado y protección de datos					x[2]

([1]) Solo si existen tareas de desarrollo de software.

([2]) Sólo si se trata de un proveedor de servicios en la nube.

El detalle si deben confluir varias de las características o si, por el contrario, es suficiente con el cumplimiento de una de ellas, se establece en el primer párrafo de cada política específica indicadas a continuación.

5.2 Seguridad física

Todos los Proveedores que presten servicio desde sus propias instalaciones, pese a que se puedan llevar a cabo actividades puntuales en las instalaciones de INERZA, deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad física:

- 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.
- Existirá algún tipo de control de las visitas, al menos en áreas de acceso público y/o de carga y descarga.
- 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.
- Si se mantiene algún tipo de copia de información responsabilidad de INERZA, 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:
  - El área especialmente protegida deberá tener un sistema de control de acceso independiente al de la sede.

- 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.
- Se mantendrá un registro de todos los accesos de personas ajenas.
- El personal externo no podrá permanecer ni ejecutar trabajos en las áreas especialmente protegidas sin supervisión.
- El consumo de alimentos o bebidas en estas áreas especialmente protegidas estará prohibido.
- Los sistemas ubicados en estas áreas deberán contar con algún tipo de protección frente a fallos de alimentación.

5.3 Auditoría de seguridad

Todos los Proveedores que tengan acceso a los sistemas de información de INERZA o que presten el servicio mediante su propia infraestructura TIC o de INERZA, independientemente del lugar en el que se preste el servicio, deberán cumplir las siguientes políticas de auditoría de seguridad:

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

5.4 Gestión de activos

Todos los Proveedores que presten servicios mediante su propia infraestructura TIC o de INERZA, independientemente del lugar en el que se preste el servicio, deberán garantizar que se cumplen, al menos, las siguientes políticas de gestión de activos:

- El Proveedor deberá contar con un registro de activos actualizado en el que se puedan identificar los activos utilizados para la prestación del servicio.
- Todos los activos utilizados para la prestación del servicio deberán tener un responsable, que se deberá asegurar de 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.
- El proveedor deberá notificar a INERZA las bajas de los activos utilizados para la prestación del servicio.
- Siempre que un activo haya contenido información responsabilidad de INERZA, 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. Si se requiere, el Proveedor aportará a INERZA certificado que confirme la eliminación segura de estos activos de información.

5.5 Arquitectura de seguridad

Todos los Proveedores que accedan a sistemas de información de INERZA y que presten servicio desde sus propias instalaciones y/o mediante su propia infraestructura TIC deberán garantizar que se cumplen, al menos, los siguientes requisitos de arquitectura de seguridad:

- Siempre que el Proveedor de servicios realice trabajos de desarrollo y/o pruebas de aplicaciones para INERZA o con datos responsabilidad de INERZA, 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 información responsabilidad de INERZA.
- Todos los accesos a los sistemas de información que alberguen o procesen información responsabilidad de INERZA deberán estar protegidos, al menos, por un cortafuegos, que limite la capacidad de conexión a ellos.
- Los sistemas de información utilizados para la prestación de servicios a INERZA deberán contar con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

5.6 Seguridad de sistemas

Todos los Proveedores que presten servicio mediante su propia infraestructura TIC, deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad de sistemas:

- Los sistemas de información que alberguen o traten información responsabilidad de INERZA deberán registrar los eventos más significativos en torno a su funcionamiento. Estos registros de actividad estarán contemplados dentro de la política de copias de seguridad de la organización.
- Los relojes de los sistemas del proveedor que procesen o alberguen información responsabilidad de INERZA estarán sincronizados entre sí y con la hora oficial.
- El proveedor del servicio garantizará que la capacidad de los sistemas de información que guarden o traten información responsabilidad de INERZA se gestiona adecuadamente, evitando potenciales paradas o malos funcionamientos de dichos sistemas por saturación de recursos.
- Los sistemas de información que alberguen o procesen información responsabilidad de INERZA estarán adecuadamente protegidos frente a software malicioso, aplicando las siguientes precauciones:
  - Se mantendrán los sistemas al día con las últimas actualizaciones de seguridad disponibles, en los entornos de prueba, desarrollo y producción.

- 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.
- 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.

- 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.
- Siempre que se utilice el correo electrónico en relación con el servicio prestado, el proveedor deberá respetar las siguientes premisas:
  - No se permitirá la transmisión vía correo electrónico de información confidencial de INERZA salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
  - No se permitirá la transmisión vía correo electrónico de información que contenga datos de carácter personal, salvo que la comunicación electrónica esté cifrada y el envío expresamente permitido.
- Siempre que para la prestación del servicio se haga uso del correo electrónico de INERZA se deberán respetar, al menos, los siguientes principios:
  - Se considerará al correo electrónico como una herramienta más de trabajo proporcionada con el fin exclusivo del servicio contratado. Esta consideración facultará a INERZA 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.
  - El sistema de correo electrónico de INERZA no deberá ser usado para enviar mensajes fraudulentos, obscenos, amenazadores u otro tipo de comunicados similares.
  - Los usuarios no deberán crear, enviar o reenviar mensajes publicitarios o piramidales (mensajes que se extienden a múltiples usuarios).
- El acceso a los sistemas de información que alberguen o procesen información responsabilidad de INERZA 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.
- Los sistemas de información que alberguen o procesen información responsabilidad de INERZA deberán contar con sistemas de control de acceso que limiten el acceso a dicha información exclusivamente al personal del servicio.
- Las sesiones de acceso a los sistemas de información que alberguen o procesen información responsabilidad de INERZA deberán bloquearse automáticamente tras un cierto tiempo de inactividad de los usuarios.

- Siempre que se haga uso de software facilitado por INERZA se deberán atender las siguientes políticas:
  - Todo el personal que acceda a los Sistemas de Información de INERZA debe utilizar únicamente las versiones de software facilitadas y siguiendo sus normas de utilización.
  - Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

5.7 Seguridad de red

Todos los Proveedores que accedan a sistemas de información de INERZA desde sus propias instalaciones y/o utilizando su propia infraestructura TIC, deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad de red:

- Las redes a través de las que circule la información responsabilidad de INERZA 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.
- Los servicios disponibles en las redes a través de las que circule la información responsabilidad de INERZA deberán limitarse en la medida de lo posible.
- Las redes que permitan el acceso a la infraestructura TIC de INERZA deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:
  - El acceso de usuarios remotos a la red de INERZA estará sujeto al cumplimiento de procedimientos de autenticación previa y validación del acceso.
  - Estas conexiones se realizarán por tiempo limitado y mediante la utilización de redes privadas virtuales o líneas dedicadas.
  - En estas conexiones no se permitirá ningún tipo de equipo de comunicaciones (tarjetas, módems, etc.) que posibilite conexiones alternativas no controladas.
- El acceso a las redes a través de las que circule la información responsabilidad de INERZA deberá estar limitado.
- Todos los equipos conectados a las redes a través de las que circule la información responsabilidad de INERZA deberán estar apropiadamente identificados, de modo que los tráficos de red puedan ser identificables.
- El teletrabajo, considerado como el acceso a la red corporativa desde el exterior, se regula mediante la aplicación de las siguientes políticas:
  - Se establecerán las medidas necesarias para la conexión segura a la red corporativa.
  - Se establecerán sistemas de monitorización y auditoría de seguridad para las conexiones establecidas.
  - 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 INERZA se deberán respetar, adicionalmente, las siguientes políticas:

- 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 INERZA o al cumplimiento de su trabajo diario.

- 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.
- Los usuarios no deberán usar el nombre, símbolo, logotipo o símbolos similares al de INERZA en ningún elemento de Internet (correo electrónico, páginas web, etc.) no justificado por actividades estrictamente laborales.
- 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.

Cualquier activo o servicio proporcionado por INERZA se utilizará sólo en el ámbito profesional para proporcionar los servicios contratados.

5.8 Trazabilidad de los sistemas

Todos los Proveedores que accedan a sistemas de información de INERZA utilizando su propia infraestructura TIC, deberán garantizar que se cumplen, al menos, las siguientes políticas de trazabilidad de uso de los sistemas:

- Se registrarán los accesos privilegiados conservándose dichos registros de acuerdo a la política de copias de seguridad de la organización.
- 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.
- Los errores y fallos registrados en la actividad de los sistemas se analizan, adoptándose las medidas necesarias para su subsanación.

5.9 Control y gestión de identidades y accesos

Todos los Proveedores con acceso a sistemas de información de INERZA, deberán garantizar que se cumplen, al menos, las siguientes políticas de control y gestión de identidades y accesos:

- 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 todos usuarios, sean estos privilegiados o no.
- Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.
- Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.
- 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.
- Las contraseñas se establecerán cumpliendo con las normas básicas de complejidad (mínimo 12 caracteres, uso de MAYÚSC y minúsc, al menos 1 carácter especial, al menos un número).

- Es recomendable utilizar las siguientes directrices para la selección de contraseñas:
  - No usar palabras conocidas, ni palabras que se puedan asociar con uno mismo, por ejemplo, el nombre.
  - 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.
  - 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.
  - No se debería utilizar el identificador de usuario como parte de la clave secreta.
- El proveedor deberá garantizar que periódicamente se constata que sólo tienen acceso a la información responsabilidad de INERZA el personal debidamente autorizado para ello.
- Ningún usuario recibirá un identificador de acceso a los sistemas de INERZA hasta que no acepte formalmente la Política de Seguridad vigente.
- Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 180 días. En caso contrario, se le podrá denegar el acceso y deberá contactar con el departamento de Soporte.
- 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 el responsable del tratamiento.
- 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 departamento de Soporte para notificar la incidencia.

5.10 Gestión de cambios

Todos los Proveedores que presten servicio utilizando su propia infraestructura TIC deberán garantizar que se cumplen, al menos, las siguientes políticas de gestión de cambios:

- Todos los cambios en la infraestructura TIC del proveedor deberán estar controlados y autorizados, garantizándose que no forma parte de la infraestructura TIC ningún componente no controlado.

- Se deberá verificar que todos los nuevos componentes introducidos en la infraestructura TIC del proveedor utilizada para la prestación del servicio funcionan adecuadamente y cumplen los propósitos para los que fueron incorporados.
- 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.
- El procedimiento de gestión de cambios deberá garantizar que se minimizan los cambios sobre los componentes críticos, limitándose a los estrictamente imprescindibles.
- 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.
- Los Proveedores deberán analizar las vulnerabilidades técnicas que presenten las infraestructuras utilizadas para la prestación del servicio, informando a INERZA de todas aquellas asociadas a los componentes críticos, con el fin de gestionar conjuntamente dichas vulnerabilidades.

5.11 Seguridad en el desarrollo

Todos los Proveedores que realicen actividades de desarrollo de software utilizando su propia infraestructura TIC o de INERZA deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad en dicha actividad:

- Todo el proceso de desarrollo de software externalizado será controlado y supervisado por INERZA, y se desarrollará de acuerdo con un proceso formal que determine las reglas a seguir.
- 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.
- Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.
- 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.
- Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.
- Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.
- Se deberá limitar la información de salida ofrecida por las aplicaciones, garantizando que sólo se ofrece aquella pertinente y necesaria.

- El acceso al código fuente de los aplicativos deberá estar limitado al personal del servicio.
- Durante las fases de desarrollo y pruebas se llevarán a cabo pruebas específicas de las funcionalidades de seguridad.
- 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.
- 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.
- Sólo se transferirán al entorno de producción aquellos aplicativos que hayan sido expresamente aprobados.

5.12 Gestión de contingencias

Todos los Proveedores que presten servicio desde sus propias instalaciones y/o mediante el uso de su propia infraestructura TIC, deberán garantizar que al menos:

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

5.13 Jurisdicción de los datos

Todo tratamiento y almacenamiento de datos en servicios en la nube, incluidas copias de seguridad y almacenamiento de logs, será exclusivamente en centros de datos localizados dentro del Espacio Económico Europeo, en cumplimiento de la normativa aplicable en materia de protección de datos, especialmente el Reglamento (UE) 2016/679 (RGPD), evitando la exposición a jurisdicciones externas que puedan comprometer los derechos de los titulares de la información.

5.14 Cifrado y protección de datos

Todos los Proveedores que traten o almacenen datos responsabilidad de INERZA deberán aplicar técnicas de cifrado mediante algoritmos tales como:

- **Cifrado Simétrico:** Uso obligatorio de AES (*Advanced Encryption Standard*) con longitudes de clave de 128, 192 o 256 bits, siendo 256 bits la opción prioritaria si está disponible.
- **Cifrado Asimétrico y Firmas Digitales**: Empleo de algoritmos RSA (mínimo 2048 bits).

- **Protocolos de Transmisión Segura**: Utilización de protocolos TLS en versión 1.2 o 1.3 para establecer canales de comunicación seguros. Siendo la versión 1.3 prioritaria si está disponible.