Cambios frente a la versión anterior	Fecha
Versión inicial.	28/08/2024

Elaborado por:	**Aprobado por:**
Salud Valor Responsable de TICs	**Nahia Val** Responsable de Procesos de Gestión

1 OBJETO

El presente documento tiene por objetivo garantizar la seguridad de los sistemas de información de CIDETEC frente a los riesgos que se puedan materializar por la prestación de servicios por parte de entidades externas.

Su finalidad es evitar posibles pérdidas o usos indebidos de información que pueda dañar o perjudicar al servicio ofrecido o a la reputación de CIDETEC. Para ello este procedimiento describe los requisitos aplicables a las entidades proveedoras, que en el desarrollo de sus funciones pudieran tener acceso a información o recursos de CIDETEC.

El objetivo concreto es proteger la confidencialidad, integridad y disponibilidad de la información y sus sistemas. Para ello, las entidades proveedoras se responsabilizarán de que las personas que trabajen para CIDETEC conozcan y se comprometan por escrito a respetar este documento.

2 ALCANCE

Este documento se aplicará a todas las actividades desarrolladas por personal de entidades proveedoras que **tengan acceso a los** sistemas **de información y/o, o que realicen desarrollos de software para CIDETEC**, vinculadas a través del correspondiente marco contractual.

- El apartado “Protocolos de seguridad generales”, será aplicable a cualquier proveedor (en el ámbito indicado anteriormente), independientemente del tipo de servicio proporcionado.
- Cada uno de los subapartados del apartado “Gestión de proveedores” 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.

3 DEFINICIONES

N/A

4 DESARROLLO

4.1 Protocolos de seguridad generales

4.1.1 Prestación de servicios a CIDETEC

1. La actividad desarrollada por la entidad proveedora se realizará de acuerdo con lo establecido en el correspondiente acuerdo regulador, así como a las normas y procedimientos establecidos a tal efecto entre CIDETEC y el proveedor.

2. La entidad proveedora proporcionará al comienzo del acuerdo contractual, la relación de perfiles, funciones y responsabilidades asociados al servicio provisto e informará puntualmente de cualquier cambio.
3. De acuerdo con lo establecido en el acuerdo, todo el personal externo que desarrolle labores para CIDETEC deberá cumplir con lo determinado en este documento.
4. La entidad proveedora deberá asegurar que todo su personal tiene la formación y capacitación apropiada para el desarrollo del servicio prestado, tanto a nivel específico en las materias correspondientes a la actividad asociada para 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 este documento.
5. Cualquier tipo de intercambio de información que se produzca entre CIDETEC y las entidades proveedoras se entenderá realizado dentro del marco contractual existente entre ambas partes de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho acuerdo.

4.1.2 Confidencialidad de la información

1. El personal externo que tenga acceso a información de CIDETEC deberá considerar que dicha información, por defecto, tiene el carácter de confidencial.
   Sólo se podrá considerar como información no confidencial aquella información 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 minimizará el número de informes en formato papel que contengan información confidencial y se mantendrán en lugar seguro y fuera del alcance de terceros.
4. El personal externo únicamente utilizará las herramientas dispuestas por CIDETEC o en mutuo acuerdo por la entidad proveedora, y en cualquier caso exclusivamente para usos profesionales.
5. Ningún colaborador deberá poseer para usos no propios de su responsabilidad, ningún material o información propia o confiada a CIDETEC.
6. En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la entidad proveedora acceda a información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicho acceso es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.
   Asimismo, el empleado deberá devolver el/los soportes inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en

cualquier caso, a la finalización de la relación de su entidad con CIDETEC. La utilización continuada de la información en cualquier formato o soporte distinto al pactado y sin conocimiento de CIDETEC no supondrá, en ningún caso, una modificación de este punto.

7. Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para CIDETEC.
8. 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.

4.1.3 Propiedad intelectual

1. Se garantizará el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.
2. Queda estrictamente prohibido el uso de programas informáticos en la infraestructura del proveedor para la prestación del servicio a CIDETEC sin la correspondiente licencia.
3. 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.

4.1.4 Intercambio de información

1. Ninguna persona debe ocultar o manipular su identidad en ninguna circunstancia.
2. La distribución de información, en soporte digital o en papel se realizará con la finalidad exclusiva de facilitar las funciones asociadas a dicho acuerdo. CIDETEC se reserva, en función del riesgo identificado, la implementación de medidas adicionales de control, registro y auditoría.
3. Con relación al intercambio de información dentro del marco contractual existente entre las partes, se considerarán no autorizadas las siguientes actividades:

    a) Transmisión o recepción de material protegido por Copyright infringiendo la Ley de Protección Intelectual.

    b) Transmisión o recepción de mensajes de naturaleza sexual, declaraciones discriminatorias raciales y cualquier otra clase de declaración o mensaje clasificable como ofensivo o ilegal.

    c) Transferencia de ficheros a terceras partes no autorizadas de material de la organización o material que sea de alguna u otra manera confidencial.

    d) Transmisión o recepción de ficheros que infrinjan la normativa de protección de datos de carácter personal.

e) Transmisión o recepción de aplicaciones no relacionadas con el negocio.

f) Participación en actividades de Internet que no estén directamente relacionadas con el servicio.

g) Todas las actividades que puedan dañar la buena reputación de CIDETEC están prohibidas.

4. Si el tratamiento de datos de carácter personal se llevase a cabo fuera de los locales de CIDETEC, deberá garantizarse el nivel de seguridad correspondiente al tipo de tratamiento.

5. La transmisión de datos de carácter personal categorizados como especialmente protegidos, se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

4.1.5 Uso apropiado de los recursos

1. El proveedor se compromete a utilizar los recursos dispuestos para la provisión del servicio de acuerdo con las condiciones para las que fueron diseñados e implantados.

2. Los recursos que CIDETEC 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. CIDETEC se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

3. Todos los equipos del proveedor que se conecten a la red corporativa (físicamente o por VPN) deberán estar homologados bajo ciertas medidas de seguridad que como mínimo deben considerarse las siguientes:
   a) Antivirus instalado y centralizado por el proveedor.
   b) Actualizaciones instaladas periódica y adecuadamente de manera centralizada.
   c) Utilización de mínimos privilegios para el usuario.

4. Cualquier fichero introducido en la red corporativa de CIDETEC o en cualquier equipo conectado a ella a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual, protección de datos de carácter personal y control de virus.

5. Al finalizar el acuerdo se deberán eliminar toda la información y software proporcionados por CIDETEC, sin retraso justificado.

6. Se prohíbe expresamente:

a) El uso de los recursos proporcionados por CIDETEC para actividades no relacionadas con el propósito del servicio.

b) La conexión a la red corporativa de CIDETEC (físicamente o por VPN) de equipos y/o aplicaciones que no estén especificados como parte del software propio de CIDETEC o bajo su supervisión.

c) Introducir voluntariamente en la red de CIDETEC 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 CIDETEC les haya asignado.

d) Intentar acceder sin autorización explícita a áreas restringidas de los Sistemas de Información de CIDETEC.

e) Intentar distorsionar o falsear los registros “log” de los Sistemas de Información de CIDETEC.

f) Intentar descifrar sin autorización explícita las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de CIDETEC.

g) Poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los recursos informáticos de CIDETEC.

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

4.1.6 Responsabilidades del usuario

1. Los proveedores de servicios deberán asegurar que el personal que desarrolla labores para CIDETEC respete los siguientes principios básicos dentro de su actividad informática:

a) Cada persona con acceso a información de CIDETEC 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 sus credenciales.

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 usuario que acceda a sistemas, en la infraestructura del proveedor, que contengan o visualicen información propiedad de CIDETEC, deberá seguir las siguientes directrices en relación con 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) Cambio de 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 usuario autorizado a acceder a información responsabilidad de CIDETEC deberá velar porque los equipos queden protegidos cuando vayan a quedar desatendidos.
4. Cualquier persona con acceso a información que pertenece a CIDETEC deberá respetar las políticas de escritorio limpio, con el fin de proteger los documentos en papel y dispositivos de almacenamiento removibles y reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.
5. Almacenar bajo llave los documentos en papel y los medios informáticos que contengan información responsabilidad de CIDETEC en mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
6. Todo el personal que acceda a la información y/o los sistemas pertenecientes a CIDETEC deberá seguir las siguientes normas de actuación:
    a) Proteger la información confidencial perteneciente o cedida por terceros a CIDETEC de toda revelación no autorizada, modificación, destrucción o uso incorrecto, ya sea accidental o no.
    b) Contar con la autorización necesaria para obtener el acceso a los sistemas de información y/o a la información necesaria.

c) Conocer, aceptar y cumplir este protocolo antes de acceder a la información y/o los sistemas de CIDETEC.

7. Ningún usuario del proveedor recibirá un identificador de acceso a los sistemas de CIDETEC hasta que dicho proveedor no acepte el presente documento y sea contratado formalmente por CIDETEC.

4.1.7 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 CIDETEC cumple las siguientes políticas:

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

   b) Ningún equipo 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 con las especificaciones del fabricante.

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

   e) Se establecerá una actualización automática de los ficheros de definición de virus.

   f) Se establecerá una política de actualizaciones de seguridad que exigirá al menos una frecuencia mensual de consulta e instalación de dichas actualizaciones.

2. Se velará especialmente por la seguridad de todos los equipos portátiles que contengan información responsabilidad de CIDETEC 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 CIDETEC.

   d) Tomando especiales precauciones en el exterior de las dependencias del proveedor para evitar la visión accidental por parte de terceras personas.

4.1.8 Retorno y Eliminación Segura de Activos de Información

1. Al finalizar el contrato con un proveedor o al finalizar el uso de un servicio de TI, se deberá asegurar el **retorno seguro** de los activos de información que pertenecen a la organización o la **eliminación segura** de dichos activos en conformidad con los estándares de seguridad establecidos.

2. El proveedor deberá proporcionar un **informe documentado** que certifique la destrucción o retorno de todos los activos de información, incluyendo copias de seguridad, datos almacenados en medios digitales y cualquier otra forma de almacenamiento de información.

3. En el caso de eliminación, los proveedores deberán utilizar métodos de destrucción que garanticen que la información no puede ser recuperada, tales como la sobreescritura segura, el borrado criptográfico o la destrucción física de los medios.

4. La **confirmación de la eliminación o retorno** de los datos debe ser entregada a la organización dentro de un plazo máximo de 30 días tras la finalización del contrato o el servicio.

4.1.9 Segregación de Clientes en Servicios Compartidos

1. Los proveedores que ofrezcan **servicios compartidos** deben garantizar que la información de la organización esté adecuadamente segregada, utilizando tecnologías y controles técnicos que aseguren la separación lógica y física de los datos.

2. Los proveedores deberán implementar medidas de **segmentación de datos** que impidan el acceso no autorizado a los datos de la organización por parte de otros clientes o usuarios.

3. La segregación de los datos debe ser revisada y verificada regularmente por la organización, a través de **auditorías técnicas** o informes proporcionados por el proveedor.

4. Los contratos con proveedores de servicios compartidos deben incluir una **cláusula de segregación** que asegure que los datos de la organización están separados de los datos de otros clientes de manera efectiva y que esta separación se mantendrá durante toda la vigencia del contrato.

4.2 Gestión de proveedores

4.2.1 Gestión del riesgo: aplicabilidad de las políticas de seguridad específicas

Todos los proveedores de IT 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 del nivel de acceso a los sistemas de información, y de las características del servicio prestado, es decir en función del riesgo.

- ✓ **Sin acceso a sistemas:** el servicio provisto no requiere de la utilización y/o acceso a los sistemas de información de CIDETEC, de modo que el personal que presta el servicio lo hace desde la infraestructura del proveedor. Dicho tipo de proveedor se divide en dos subcategorías:
  - ➢ **Con acceso a información de CIDETEC:** el proveedor presta el servicio desde su infraestructura almacenando y/o tratando información propiedad de CIDETEC.
  - ➢ **Sin acceso a información de CIDETEC:** el proveedor presta el servicio sin tratar y/o almacenar información de CIDETEC.
- ✓ **Gestión remota de aplicaciones de CIDETEC**: el servicio prestado requiere de la utilización de los sistemas de información de CIDETEC de modo que el personal que presta el servicio dispone de cuentas de usuario que les permiten acceder de forma remota (no se requiere el acceso a la red corporativa) a las aplicaciones corporativas.
- ✓ **Con acceso a red corporativa con nivel usuario**: el servicio prestado requiere el acceso a través de la red corporativa (físicamente o por VPN) a alguno de los sistemas de información de CIDETEC con privilegios de usuario.
- ✓ **Con acceso a red corporativa "site to site":** el servicio prestado requiere del intercambio de información entre la red interna de CIDETEC y la red interna del tercero contratado. En esta categoría también aplican aquellos usuarios que requieran de acceso privilegiado a los sistemas de información de CIDETEC, 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, los protocolos específicos recogidos en los apartados que se indican en la siguiente tabla:

	Sin acceso a sistemas / Sin acceso a información	Sin acceso a sistemas / Con acceso a información	Gestión remota aplicaciones	Acceso red corporativa a nivel usuario	Acceso red corporativa "site to site"
Auditoría de seguridad/informes	NO	NO	SI	SI	SI
Comunicación de incidencias	SI	SI	SI	SI	SI
Seguridad de sistemas	NO	SI	SI	NO	SI
Seguridad de red	NO	SI	NO	NO	SI
Trazabilidad de uso de los sistemas	NO	SI	NO	SI	SI
Control y gestión de identidades y accesos	NO	SI	NO	NO	SI
Seguridad en desarrollo	NO	NO	*NO*	SI	SI

4.2.1.1 Auditoria de Seguridad/Informes

Todos los proveedores de servicios que aplique, según su tipología deberán cumplir las siguientes políticas de auditoría de seguridad:

1. El proveedor deberá permitir a CIDETEC llevar a cabo al menos una auditoría de seguridad del servicio al año,en caso de ser necesario, colaborando con el equipo auditor y facilitando todas las evidencias y registros requeridos. Como alternativa a las auditorías, el proveedor podrá proveer de informes de seguimiento a CIDETEC.

4.2.1.2 Comunicación de incidencias

Todos los proveedores de servicios que aplique según su tipología deberán cumplir las siguientes políticas de comunicación de incidencias:

1. Todo el personal asignado al servicio deberá ponerse en contacto con CIDETEC a través del buzón de correo electrónico "svalor@cidetec.es", en caso de que detecte cualquier incidencia relacionada con la seguridad de la información o los recursos de CIDETEC.

En caso de considerarse una incidencia crítica, además de comunicarse por dicho correo electrónico, se deberá comunicar al interlocutor de CIDETEC, quien se pondrá en contacto con el CAU interno.

4.2.1.3 Seguridad de sistemas

Todos los servicios que aplique según su tipología 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 CIDETEC 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. El proveedor del servicio garantizará que la capacidad de los sistemas de información que guarden o traten información responsabilidad de CIDETEC se gestiona adecuadamente, evitando potenciales paradas o malos funcionamientos de dichos sistemas por saturación de recursos.
3. Los sistemas de información que alberguen o procesen información responsabilidad de CIDETEC 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.
4. 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.
5. Siempre que se utilice el correo electrónico en relación con el servicio prestado, el proveedor deberá respetar las siguientes premisas:
    a) No se permitirá la transmisión vía correo electrónico de información confidencial de CIDETEC salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
    b) No se permitirá la transmisión vía correo electrónico de información que contenga datos de carácter personal de nivel alto, salvo que la comunicación electrónica esté cifrada y el envío este expresamente permitido.
6. El acceso a los sistemas de información del proveedor que alberguen o procesen información responsabilidad de CIDETEC 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.

7. Los sistemas de información que alberguen o procesen información responsabilidad de CIDETEC deberán contar con sistemas de control de acceso que limiten el acceso a dicha información exclusivamente al personal del servicio.

8. Siempre que se haga uso de software facilitado por CIDETEC 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.

Está prohibido desinstalar cualquiera de los programas instalados por CIDETEC.

4.2.1.4 Seguridad de red

Todos los proveedores de servicios que aplique según su tipología deberán garantizar respecto a la información responsabilidad de CIDETEC 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 CIDETEC deberán estar apropiadamente protegidas, debiéndose cumplir las siguientes premisas:

    a) El acceso de usuarios remotos a la red de CIDETEC 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 (hubs, switches, 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.

4.2.1.5 Trazabilidad de uso de los sistemas

Todos los proveedores de servicios que aplique según su tipología 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 con 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 con la política de copias de seguridad de la organización.
3. Los errores y fallos registrados en la actividad de los sistemas se analizan, adoptándose las medidas necesarias para su subsanación.

4.2.1.6 Control y gestión de identidades y accesos

Todos los proveedores de servicios que aplique según su tipología 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 CIDETEC:

1. Todos los usuarios con acceso a un sistema de información dispondrán de una autorización de acceso unipersonal.
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. Debe existir una política de seguridad de contraseñas.
6. El proveedor deberá garantizar que periódicamente se constata que sólo tienen acceso a la información responsabilidad de CIDETEC el personal debidamente autorizado para ello.

4.2.1.7 Seguridad en Desarrollo

Todos los proveedores de servicios que aplique según su tipología 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 será controlado y supervisado por CIDETEC y deberán disponer de una metodología de desarrollo seguro que involucre todas las

fases del ciclo de vida de desarrollo, no solo a nivel de código, sino también a nivel de gestión y protección del código.

2. Deberán incorporar 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 los entornos de pruebas y desarrollo sólo se utilizarán datos reales cuando hayan sido apropiadamente disociados o siempre que se pueda garantizar que las medidas de seguridad aplicadas sean equivalentes a las existentes en el entorno de producción.
11. Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.
12. Se establecerá un sistema de control de versiones que permitan la trazabilidad sobre el desarrollo del código.
13. Los entornos con los que se lleven a cabo los desarrollos deberán estar aislados entre sí y también aislados de los entornos de producción en los que se albergue o procese la información.

5 REFERENCIAS

6 ANEXOS