sescam
Servicio de Salud de Castilla-La Mancha

Director Gerente

FECHA: 18 de noviembre de 2009.

ASUNTO: Circular nº 3/2009.
Políticas del Área de Tecnologías de la Información del Servicio de Salud de Castilla - la Mancha

AMBITO: Direcciones Generales y Secretaría General
Gerencias de Atención Primaria, Atención Especializada, de Área, de Urgencias, Emergencias y Transporte Sanitario y de Inspección de Servicios Sanitarios y Prestaciones.
Oficinas Provinciales de Prestaciones.

ORIGEN: Secretaría General.

La necesidad de garantizar el adecuado uso de los sistemas de información y del equipamiento informático que el Servicio de Salud de Castilla - La Mancha (SESCAM) pone a disposición de sus trabajadores para el desempeño de sus funciones, hace necesario el establecimiento de políticas de diversa índole dentro del ámbito de las Tecnologías de la Información y las Comunicaciones con el objetivo de conseguir que dicho uso se haga de manera correcta y segura.

El Área de Tecnologías de la Información del Sescam ha elaborado una serie de políticas de diversa índole sobre todos los aspectos propios de su ámbito, redes y sistemas de información. Cada una de estas políticas va dirigida a un conjunto de trabajadores y, por lo tanto, es imprescindible que dichos trabajadores sepan de su existencia y de la obligatoriedad de su cumplimiento.

En función de lo anterior, la Dirección Gerencia del SESCAM establece las siguientes

C/. Huérfanos Cristinos, 5 • 45071 TOLEDO

INSTRUCCIONES

Primera.- Objeto y definición.

La presente Circular tiene por objeto impartir instrucciones sobre difusión y cumplimiento de las políticas de tecnologías de la información y las comunicaciones del SESCAM.

A los efectos de la presente Circular se entenderá por *política de tecnologías de la información y las comunicaciones* aquél documento definido como tal por el Área de Tecnologías de la Información en el que se recojan un conjunto de indicaciones, directrices, medidas, procedimientos, etc... que deben ser respetados para la mejor gestión y uso de los medios informáticos en el ámbito del SESCAM.

Segunda.- Ámbito de aplicación.

La presente Circular es de aplicación en todo el ámbito del SESCAM. En concreto comprenderá los Servicios Centrales, las Oficinas Provinciales de Prestaciones, las Gerencias de Atención Primaria, Atención Especializada, de Área, de Urgencias, Emergencias y Transporte Sanitario y de Inspección de Servicios Sanitarios y Prestaciones.

Tercera.- Difusión de las políticas del Área de Tecnologías de la Información

Las políticas de tecnologías de la información y las comunicaciones existentes y las que se desarrollen en lo sucesivo, serán objeto de publicación en la intranet del SESCAM (http://intranet.sescam.jclm.es/politicasTIC/)

En el momento de la aprobación de la presente Circular, las políticas elaboradas y publicadas son:

- Política de Seguridad Global del SESCAM (Se incorpora como anexo)
- Política para la Gestión de Herramientas Anti-malware
- Política para la Gestión de Incidencias de Seguridad
- Política para la Adquisición, Desarrollo y Mantenimiento de aplicaciones desde el punto de vista de la seguridad
- Política para la Gestión de la Responsabilidad sobre los activos
- Política en relación a los Recursos Humanos desde el punto de vista de la seguridad
- Política para la Gestión de las Operaciones y las Comunicaciones
- Política para los Accesos Remotos desde el punto de vista de la seguridad
- Política de Funciones y Responsabilidades de los usuarios
- Política para la Gestión de la Continuidad del Negocio
- Política para el Control de la Seguridad Física
- Política para el Control de Acceso Lógico
- Política para el Cumplimiento Legal de las medidas de seguridad
- Política para la Organización de la Seguridad de la Información
- Política de Desarrollo de Aplicaciones
- Política de Comunicaciones para Accesos Externos
- Política de Comunicaciones para Telefonía Móvil
- Política de Comunicaciones para la Publicación Web
- Política de Comunicaciones para obras en las Gerencias de Atención Especializada
- Política de Comunicaciones para obras en las Gerencias de Atención Primaria
- Política de Comunicaciones para el Acceso a la Plataforma de Envío de SMS

C/. Huérfanos Cristinos, 5 • 45071 TOLEDO

- Política de Comunicaciones para la Conectividad a las Infraestructuras y Servicios de Telecomunicaciones Corporativos
- Política de Comunicaciones para el Acceso del Sistema de Videoconferencia
- Política de Comunicaciones para el Acceso a la Plataforma de Voz Corporativa
- Política de Gestión de Antivirus
- Política de Copias de Seguridad
- Política de Estándares de Sistemas
- Política de Explotación de Datos
- Política de Firma Electrónica
- Política de Gestión de Incidencias de Sistemas
- Política de Gestión de Usuarios
- Política de Integración de Sistemas
- Política de Directorio Electrónico (LDAP)
- Política de Mantenimiento de Centros de Procesos de Datos (CPD's)
- Política de Puestas en Producción de aplicaciones
- Política de Publicación de Contenidos en la Cartelería Digital
- Política de Retirada de Material Informático
- Política de Suministro de Material Informático
- Política de Definición de Estándares

Además de su difusión a través de la inserción en la intranet del SESCAM, el Área de Tecnologías de la Información enviará de manera personalizada las nuevas políticas que se elaboren, así como sus sucesivas versiones, a los usuarios que deban conocerlas.

Para la difusión de aquellas políticas que resulten de especial trascendencia e impacto en la organización, el Área de Tecnologías de la Información podrá realizar cursos de formación online, de forma que se facilite la incorporación de las buenas prácticas en el uso diario.

Cuarta.- Obligaciones con respecto a las políticas de todo el personal al que van dirigidas

Todos los grupos de usuarios a los que vaya dirigida una determinada política están obligados a cumplir con las directrices y especificaciones definidas en el documento.

El Área de Tecnologías de la Información analizará periódicamente el grado de cumplimiento de las políticas con el fin de detectar aquellas deficiencias que puedan afectar a la calidad de las redes y sistemas de información y a tal efecto emitirá un informe donde se indicarán las medidas a llevar a cabo para corregir las deficiencias observadas.

Quinta.- Efectos.

La presente Circular será de aplicación a partir del día siguiente al de su firma.

Lo que se participa para su conocimiento y cumplimiento.

En Toledo, 18 de octubre de 2009

CONSEJERÍA DE SALUD Y BIENESTAR SOCIAL Castilla-La Mancha sescam

EL DIRECTOR-GERENTE

Ramón Gálvez Zaloña

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SESCAM

Versión: ***1.0***
Identificación: ***Política de Seguridad de la Información del SESCAM***

INDICE :

HOJA DE CONTROL DE CAMBIOS EN EL DOCUMENTO

Fecha	Versión	Cambios (respecto a la versión anterior)
25/3/2009	1.0	- Documento base

Versión	Realizado / Modificado por	Revisado/Modificado por	Modificado/Aprobado por
1.0	Consultores Seguridad	Grupo Seguridad	Grupo Seguridad

1 INTRODUCCIÓN.

La "Política de Seguridad de la Información" pasa por ser el documento que formaliza el compromiso legal y ético del SESCAM con relación a establecer la Seguridad de la Información como uno de sus principios fundamentales.

Así, el SESCAM adquiere la responsabilidad activa de promover y apoyar la instauración de medidas técnicas, organizativas y de control que garanticen la integridad, disponibilidad y confidencialidad de la información que concierne a los ciudadanos a los que da servicio, personal propio, entidades externas colaboradoras y organismos oficiales competentes.

Así mismo, se presentan los objetivos y las responsabilidades necesarias para proteger los activos que conforman los Sistemas de Información, imprescindibles para el manejo de dicha información, garantizando igualmente su integridad, disponibilidad y confidencialidad, cumpliendo con el marco legal vigente y respetando las directrices, normas y procedimientos que oportunamente se establezcan.

La aceptación de este propósito sienta las bases para, por un lado, documentar de forma clara y concreta las directrices establecidas por el SESCAM en materia de seguridad y, por otro, que sean conocidas y practicadas por todo el personal, tanto propio como externo, implicado.

2 OBJETIVO.

El objetivo del presente documento es el de establecer las directrices esenciales que garanticen la protección eficaz y eficiente de los Sistemas de Información del SESCAM, con el fin de preservar la información de la que es responsable y cumplir las leyes que afectan al tratamiento de la misma.

En definitiva, el SESCAM no persigue otro objetivo que garantizar que la información sea segura, entendiendo que la información es segura cuando su confidencialidad, su integridad, su disponibilidad, así como la de los sistemas utilizados en su tratamiento, adquieren un nivel de riesgo aceptable.

3 ALCANCE.

Esta política es de aplicación a toda la información del Servicio de Salud de Castilla-La Mancha (SESCAM), con independencia del atributo que le afecte, la forma en la que se presente o el lugar en el que se encuentre. La política es aplicable, igualmente, en todas fases del ciclo de vida de la información (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción).

Cualquier norma interna que trate algún aspecto particular de la seguridad de la información del SESCAM debe nacer de esta política.

4 DEFINICIONES.

- **Activo:** Recurso del Sistema de Información necesario para que éste funcione correctamente y que tiene valor para la organización.
- **Amenaza:** Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales.
- **Confidencialidad:** Dimensión de la seguridad por la cual se garantiza que sólo las personas, entidades o procesos autorizados pueden acceder a la información.
- **Control:** Acción, procedimiento, normativa o dispositivo, físico o lógico, que permite reducir el riesgo.
- **Disponibilidad:** Dimensión de la seguridad por la cual se garantiza que los usuarios autorizados acceden a la información, y a los recursos o servicios que la manejan, siempre que lo requieran.
- **Impacto:** Consecuencia sobre un activo tras la materialización de una amenaza.
- **Información:** Todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma.
- **Integridad:** Dimensión de la seguridad por la cual se garantiza que la información no pueda ser o no ha sido modificada o alterada por personas, entidades o procesos no autorizados.
- **Riesgo:** La probabilidad o potencialidad de que una vulnerabilidad sea explotada por una amenaza.
- **Sistema de Gestión de la Seguridad de la Información (SGSI):** Elemento del sistema de gestión, que se basa en la evaluación del riesgo para establecer, implantar, desarrollar, controlar, revisar, mantener y mejorar la Seguridad de la Información.
- **Sistema de Información:** Conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita manejar información.
- **Vulnerabilidad:** Debilidad, atributo o pérdida de control que permitiría o facilitaría la materialización de una amenaza.

5 REFERENCIAS.

Los documentos siguientes, en su última edición / revisión, servirán como referencia para la definición de la presente política:

- ISO/IEC 27002: "Código de buenas prácticas para la Gestión de Seguridad de la Información".

- ISO/IEC 27001: "Especificaciones relativas a la Gestión de la Seguridad de la Información".

6 POLITICA DE SEGURIDAD.

La información es un concepto abstracto e intangible que se genera, distribuye, almacena, procesa, transporta, consulta o destruye mediante elementos tangibles. Estos elementos son: las personas, los documentos, los sistemas de información, las redes de telecomunicaciones, las instalaciones y las empresas. De acuerdo con ello, la protección de la información se realizará mediante la aplicación y supervisión de medidas de seguridad dirigidas a estos últimos elementos.

El objetivo fundamental que persigue la gestión de la seguridad de la información es garantizar que los riesgos a los que se encuentra expuesta la información sean conocidos, asumidos, gestionados y minimizados. Todo ello de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan, tanto en los propios riesgos, como en el entorno y las tecnologías.

Para ello se debe:

- Establecer los requisitos de seguridad, de obligado cumplimiento, de los Sistemas de Información del SESCAM.

- Identificar los controles de gestión, entorno, operacionales y técnicos que se necesitan para cumplir con los requisitos de seguridad.

El documento de Política de Seguridad de la Información se encuentra aprobado por la Dirección Gerencia y el Grupo de Trabajo de Seguridad, y se publica para que sea conocido por todo el personal (propio y externo) que maneja, de forma directa o indirecta, la información propiedad del SESCAM.

La aplicación del presente documento es de obligado cumplimiento de forma directa en todos los centros, sedes, gerencias, y oficinas del SESCAM.

La Política de Seguridad de la Información será revisada y actualizada cada dos años y, excepcionalmente, cuando se produzcan cambios significativos en el ámbito del SESCAM.

6.1 Análisis y Gestión del Riesgo.

Los riesgos a los que se encuentran expuestos los elementos que manejan la información del SESCAM deben analizarse. Los resultados de estos análisis deberán determinar las acciones de gestión de la seguridad más apropiadas para minimizarlos y priorizar las mismas. Para ello se seguirá la metodología MAGERIT 2.0 para el Análisis y la Gestión del Riesgo.

El análisis de los riesgos debe realizarse de manera periódica para contemplar los cambios en los requisitos de seguridad, así como los cambios que se produzcan en los activos, amenazas, vulnerabilidades e impactos. Por su parte, la gestión del riesgo debe ser llevada a cabo de una manera metódica y capaz de generar unos resultados comparables y reproducibles.

Tras la obtención de los resultados se debe decidir cuando un riesgo es aceptable y cuando no, siempre según los principios de servicio del SESCAM.

Para cada uno de los riesgos identificados, se procederá a desarrollar el tratamiento más acertado en base a la gestión de riesgos.

6.2 Estructura Organizativa de la Seguridad.

El SESCAM debe crear una estructura organizativa para iniciar, conseguir y mantener la implantación de los objetivos de Seguridad de la Información en todo su marco de aplicación.

Dicha estructura organizativa debe estar formada por:

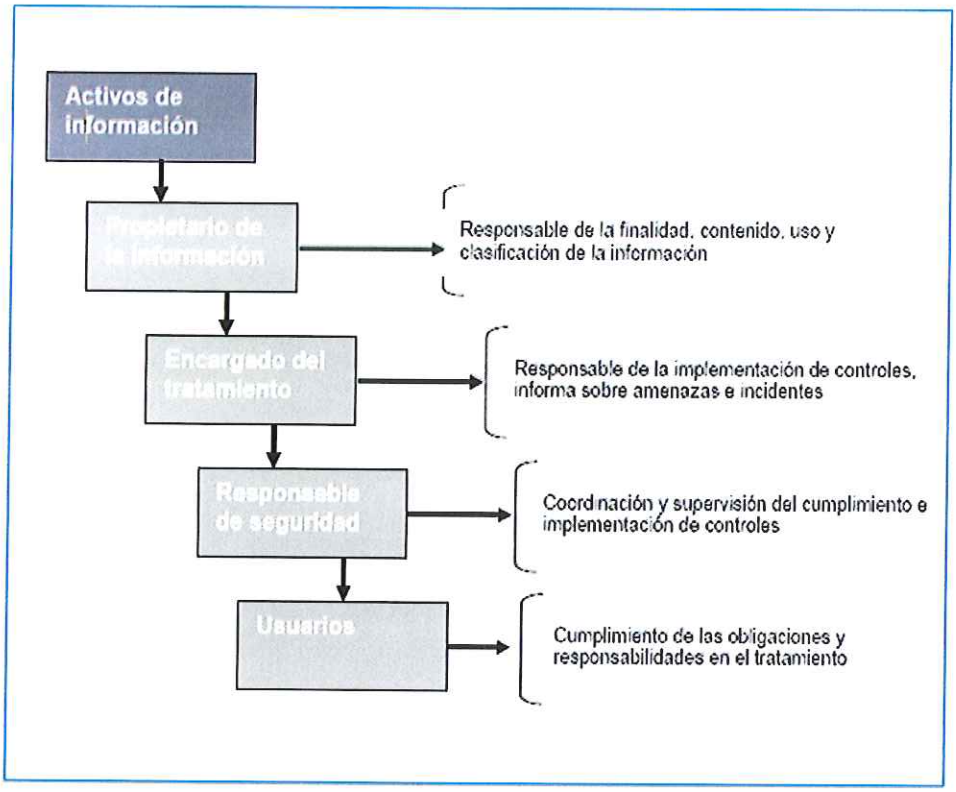
- El Grupo de Trabajo del Seguridad, compuesto por representantes de todas las áreas necesarias para coordinar las iniciativas asociadas a la seguridad de la información. Adicionalmente, debe asumir las funciones de aprobación de las políticas, normativas y procedimientos de seguridad, garantizar la disponibilidad de los recursos dedicados a la seguridad de la información y mantenerse informado del nivel de seguridad existente en las diferentes áreas del SESCAM.

- El Equipo de Seguridad, dependiente de la función de organización e independiente, al menos, de producción y desarrollo. Debe estar formada por el Responsable de Seguridad y los Consultores de Seguridad. Su función es la de gestionar la seguridad de la información, de forma interna, en el SESCAM.

Adicionalmente a los requerimientos técnicos, funcionales y económicos establecidos en los contratos de prestación de servicios por parte de terceros, se deben incluir requerimientos específicos de seguridad relativos al manejo y protección de la información por aquellos que llevan a cabo su instalación, configuración, mantenimiento o eliminación.

De forma análoga, se establecerán estos requisitos para todos los contratos de externalización de servicios. Es responsabilidad del personal del SESCAM entender los riesgos derivados del proceso de externalización y asegurar que existe una gestión eficaz de los mismos.

De manera general, la distribución de responsabilidades sobre la información del SESCAM que se maneja puede entenderse mediante el siguiente esquema:



6.3 Mantenimiento y Difusión del Cuerpo Normativo de Seguridad.

El Responsable de Seguridad del SESCAM debe desarrollar el Cuerpo Normativo de seguridad, formado por políticas, normativas, estándares y procedimientos, con la finalidad de asegurar que el marco de actuación de la seguridad se extiende a todos sus ámbitos. La presente Política de Seguridad establece las directrices generales de seguridad que se deben definir en los subsiguientes componentes del Cuerpo Normativo.

Es necesario que el Cuerpo Normativo de seguridad sea completo y proporcione suficiente información para definir y establecer las necesidades de protección de la información y los activos asociados a la misma en el ámbito del SESCAM.

El Cuerpo Normativo de seguridad debe actualizarse en función de los cambios producidos en el marco legal vigente, inclusión de resultados relevantes tras auditorias o análisis de riesgos, sugerencias de mejora, etc.

Adicionalmente, se debe diseñar el procedimiento necesario para la divulgación del Cuerpo Normativo de seguridad, con el objetivo de que sea conocido y aplicado por todos los usuarios afectados por el alcance de aplicación de la Política de Seguridad, concienciándolos convenientemente con relación a la seguridad de la información.

6.4 Gestión de los Activos.

Es responsabilidad del SESCAM mantener un inventario de los activos de información relevantes que son de su propiedad, velando porque exista un responsable y custodio para cada uno de los mismos. Este inventario debe ser actualizado de forma regular.

Con la finalidad de establecer un nivel de seguridad y tratamiento de la información adecuados, los activos de información deben ser clasificados conforme a su sensibilidad y criticidad. A tal fin, se deben desarrollar las guías de clasificación de la información y las medidas de protección asociadas.

6.5 Seguridad ligada al Personal.

Todos el personal propio y subcontratado, entidades colaboradoras y, en última instancia los usuarios externos, deben recibir la formación apropiada para el uso correcto de los servicios y sistemas que manejan información del SESCAM, incluyendo requerimientos de seguridad (procedimientos de inicio de sesión seguro, uso apropiado de software, acceso a información…) y responsabilidades legales.

Los usuarios deben ser conscientes de la importancia de la seguridad en los Sistemas de Información del SESCAM. La seguridad eficaz depende, en parte, de que los usuarios sepan lo que se espera de ellos y cuáles son sus responsabilidades. Éstos deben conocer los argumentos asociados a las medidas de seguridad física y lógica establecidas, así como las consecuencias de violar las normas seguridad.

6.6 Seguridad Física y del Entorno.

Los Sistemas de Información del SESCAM, así como los soportes de almacenamiento que residan en sus edificios y en los de los proveedores de servicio o terceros, deben estar protegidos contra el daño físico o el hurto, utilizando para ello mecanismos de control de acceso físico que aseguren que únicamente el personal autorizado tiene acceso a los mismos.

Con esta finalidad, los Sistemas de Información del SESCAM deben estar ubicados en áreas de acceso restringido, con diferentes niveles de seguridad, a las cuales únicamente pueda acceder personal debidamente autorizado.

Por su parte, los equipos y la información que manejan deben estar adecuadamente protegidos frente a amenazas físicas o ambientales, sean éstas intencionadas o accidentales.

6.7 Gestión de Comunicaciones y Operaciones.

El SESCAM debe establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos de tratamiento de información. Esto incluye el desarrollo de instrucciones apropiadas de operación y de procedimientos de respuesta ante incidencias.

Se debe instaurar la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

El software y los recursos de tratamiento de información son vulnerables a la introducción de malware dañino, como virus informáticos, gusanos de la red, troyanos y bombas lógicas. Los usuarios deben conocer los peligros que entraña el software dañino o no autorizado, y deben existir controles y medidas especiales para detectar o evitar su introducción en puestos de trabajo, servidores y pasarelas de conexión a redes públicas o privadas. En particular, es esencial que se tomen precauciones para detectar o evitar los virus informáticos en las estaciones de trabajo. Es de obligado cumplimiento la actualización periódica y regular de los mecanismos antivirus para todo el sistema del SESCAM.

Se deben establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo. Para ello se realizarán copias de respaldo, pruebas de restauración, registros de eventos o fallos y monitorización del entorno de los equipos cuando proceda.

La gestión de la seguridad de las redes que cruzan los límites del SESCAM requiere una atención especial que se concreta en controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas. Se deben instaurar los controles necesarios para impedir la suplantación del emisor y/o modificación o pérdida de la información transmitida, tanto en las comunicaciones con sistemas situados en las redes internas como con aquellos sistemas externos, independientemente de la plataforma, protocolos o aplicaciones que las soporten.

Se deben implementar los procedimientos adecuados para proteger los documentos, soportes informáticos (discos, cintas, etc., datos de entrada/salida y documentación del sistema frente a daño, robo y acceso no autorizado. El almacenamiento, manipulación, transporte, destrucción o desecho de cualquier activo de información del SESCAM que contenga información sensible debe garantizar la imposibilidad de acceso o recuperación de su contenido por parte de personal no autorizado.

Todos los intercambios de información y software entre el SESCAM y otras organizaciones, deberán cumplir con la legislación vigente y se deben realizar sobre la base de acuerdos formales. También se deberán considerar las implicaciones de seguridad asociadas al correo electrónico e intercambio de datos electrónicos, así como los requerimientos para las medidas y controles de seguridad.

Por último, se debe instaurar la estructura organizativa multidisciplinar necesaria para acometer la resolución de incidentes de seguridad.

6.8 Control de Accesos.

Los permisos de acceso a las redes, sistemas y a la información que estos soportan se otorgarán de modo que los usuarios tengan acceso únicamente a los recursos e información necesarios para el desempeño de sus funciones.

Se deben establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios. Estos procedimientos cubrirán todas las etapas del ciclo de vida del acceso a usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios. Se prestará especial atención al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema.

Todos los accesos realizados a los Sistemas de Información del SESCAM por los usuarios registrados llevarán asociado un proceso de identificación, autenticación y autorización. Se establecerán mecanismos de registro, monitorización de acceso y uso de los sistemas.

Las credenciales de acceso de cada usuario serán personales e intransferibles. Toda persona registrada que disponga de credenciales de acceso será responsable de mantener su confidencialidad y asegurar su correcto uso. Se establecerán los mecanismos necesarios en los sistemas para impedir la visualización de las credenciales por parte de terceras personas.

Debido a que una protección efectiva necesita la cooperación de los usuarios autorizados, los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de la efectividad de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

El acceso a los servicios desde redes externas e internas debe ser controlado de forma tal que se asegure que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios.

El acceso remoto a los Sistemas de Información del SESCAM desde redes públicas debe garantizar la confidencialidad de la información que se transmite, así como la identidad de los usuarios autorizados a hacer uso del servicio de acceso remoto, mediante mecanismos de autenticación fuerte.

Se debe restringir el acceso a los ordenadores de modo que sólo se permita su utilización a usuarios autorizados. Los ordenadores que atienden a múltiples usuarios deberían ser capaces de identificar y verificar la identidad de cada usuario autorizado y, si procede, el terminal o la ubicación física del mismo.

Con la finalidad de detectar y reaccionar ante comportamientos sospechosos o inesperados, se deben establecer sistemas de registro de actividades que almacenen los datos generados por las actividades de sistemas, aplicaciones y usuarios en los activos de información del SESCAM.

En los casos que aplique, se establecerán normativas, procedimientos y medidas técnicas específicas para la protección de equipos portátiles y accesos remotos del tipo de teletrabajo.

6.9 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

El desarrollo y mantenimiento de sistemas y aplicaciones debe contener los controles y registros apropiados para garantizar la correcta implementación de las especificaciones de seguridad y se llevará a cabo teniendo en cuenta las mejores prácticas de seguridad en materia de programación.

Especialmente, se usarán sistemas y técnicas criptográficas (cifrado, firma digital, no-repudio) para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

La información residente en los Sistemas de Información del SESCAM debe estar protegida contra modificaciones no autorizadas empleando mecanismos que aseguren la integridad de la misma.

El Equipo de Seguridad deberá proveer las guías, estándares, recomendaciones y procedimientos necesarios para facilitar la inclusión de la seguridad durante las etapas del ciclo de vida de desarrollo, tales como uso de controles criptográficos, gestión de claves, programación segura, etc.

Los entornos del ciclo de vida del desarrollo informático deben estar convenientemente separados o segmentados en todos y cada uno de los sistemas. Asimismo, y con la finalidad de evitar el acceso

o divulgación de datos que residan en los entornos, se debe controlar el intercambio de datos reales entre el entorno de producción y el resto de entornos.

En los entornos de preproducción, pruebas o desarrollo, para aplicaciones, programas, productos, etc., deben estar disponibles juegos de datos, preparados específicamente, donde los datos de carácter personal hayan sido disociados o enmascarados.

6.10 Continuidad de Negocio.

Debe existir un proceso de gestión de continuidad de actividades para garantizar la recuperación de los procesos críticos soportados por el SESCAM ante un caso de desastre. Se proyectará reducir el tiempo de indisponibilidad del servicio a niveles aceptables mediante la adecuada combinación de controles de carácter organizativo, tecnológico y procedimental, tanto preventivos como de recuperación.

Este proceso es responsabilidad del Equipo de Seguridad y se desarrollará mediante un Plan de Continuidad de Negocio que debe ser probado de forma periódica y regular, y que debe mantenerse actualizado en todo momento. Para ello, se evaluará el riesgo y el impacto asociado ocasionado por la ausencia de continuidad de los sistemas de información que den soporte o estén implicados en la actividad del SESCAM.

6.11 Conformidades.

El SESCAM adquiere la responsabilidad de cumplir con la legislación vigente relativa a la Seguridad de la Información. El Responsable de Seguridad debe identificar los estatutos relevantes, regulaciones, leyes y requisitos contractuales que afecten directa o indirectamente a la seguridad de los activos de información que pertenecen al SESCAM.

Especialmente se atenderá a lo dispuesto en el Título VIII, sobre las medidas de seguridad en el tratamiento de datos de carácter personal, del REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.