Políticas, Normas, Procedimientos y Protocolos de seguridad

Políticas, normativas, procedimientos y protocolos de seguridad.

2013.

Autores:

Emilio Sánchez Pérez

Impresión.

Depósito Legal.

Diseño.

PRESENTACIÓN DEL MANUAL

EAP

Políticas, normativas, procedimientos y protocolos de seguridad

Políticas, normativas, procedimientos y protocolos de seguridad.

Unidad 1: Introducción.

- Contexto actual de la Política de Seguridad y Esquema Nacional de Seguridad.

Unidad 2: Contexto. Política de Seguridad.

- Concepto de política de seguridad.
- Principios de protección de la información
- Desarrollo de la política de seguridad

Unidad 3: Contexto. Normativa de Seguridad.

- Concepto de normativa de seguridad.
- Desarrollo de la norma de seguridad.

Unidad 4: Contexto. Procedimientos de Seguridad.

- Concepto de procedimientos de seguridad.
- Ejemplos de procedimientos de seguridad.

Unidad 5: Contexto. Protocolos de seguridad

- Concepto de protocolo de seguridad.
- Portal CSIRT

Unidad 6: Marco Legal

- Decreto Legislativo 1/2001

Protección de datos personales y su procesamiento.

Otras leyes de interés.

Introducción del Módulo y Objetivos o Expectativas de aprendizaje.

En el módulo de políticas, normativa, procedimientos y protocolos de seguridad se va a abordar el valor de la información que se encuentra en nuestro equipos, la necesidad de la existencia de estos documentos de seguridad, una forma de organizar la información en la CARM siempre asegurando la confidencialidad, integridad y disponibilidad de la información manejada. Veremos la justificación de porqué es necesario tener una o varias políticas de seguridad definidas, porqué es necesario establecer normas y procedimientos, quien/es los gestiona/n, quien/es los aprueba/n...

Una vez que se haya finalizado el módulo, el usuario debería tener una visión global de lo que es una política de seguridad, de que es una normativa así como un procedimientos y un protocolo de seguridad, teniendo clara su responsabilidad como participe de la seguridad de la información dentro de la CARM. Donde se puede consultar esta información y a quien acudir en caso de algún problema que esté relacionado con la disponibilidad, confidencialidad e integridad de la información con la que diariamente el usuario trabaja. Además el usuario debiera ser capaz de identificar los problemas básicos que pudieran activar cualquier protocolo de seguridad definido en el ámbito de la CARM/DGPIT.

Por último el usuario tendrá que conocer sobre qué bases legales se apoya su trabajo diario en relación con la seguridad de la información. La profundización en este aspecto se deja en manos del usuario.

1. Contenido

2. Introducción.

"Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad. Cuando algo sucede, nos lamentamos de no haber invertido más… Más vale dedicar recursos a la seguridad que convertirse en una estadística".

El R.D. 3/2010, de 8 de Enero, regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica que persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. En este contexto, la seguridad de la información tiene como objetivo proteger la información y los servicios reduciendo los riesgos a los que están sometidos hasta un nivel que resulte aceptable dado que siempre podrá haber eventos o situaciones no previsibles que puedan producir incidentes.

La seguridad de esta información es la que desde el equipo de respuestas a incidentes de seguridad informática, en adelante CSIRT, estamos enfocados a proteger preventiva y proactivamente apoyándonos en las políticas, normas, procedimientos y protocolos de seguridad establecidos de manera que la información de la CARM no se vea comprometida y todos los usuarios puedan identificar posibles fugas de información o mal uso de la misma.

Las tres principales dimensiones que preserva la seguridad de la información de una organización son la disponibilidad, la integridad y la confidencialidad y es el CSIRT en colaboración con todos los usuarios de la CARM quienes tutelarán esta información e intentarán que estas tres dimensiones anteriormente citadas no se vean comprometidas, pudiendo estar involucradas además otras propiedades como la autenticidad y la trazabilidad de la información. A continuación se explican estos conceptos;

Disponibilidad: La disponibilidad es la propiedad de ser accesible y utilizable por la demanda de una entidad autorizada. ¿Puedo acceder a la información siempre?

Integridad: La integridad es la propiedad de salvaguardar la exactitud y la completitud de los activos de información. ¿Los datos han sido modificados?

Confidencialidad: La confidencialidad es la propiedad de la información por la que esta no se muestra disponible o revelada para individuos, entidades o procesos no autorizados. ¿Alguien accede a documentación que no debe?

Autenticidad: Con el término autenticidad se hace referencia al aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red. El objetivo que se pretende es la comprobación de que dichos datos o información provienen realmente de la fuente que dice ser.

El problema del control de autenticidad dentro de los sistemas de información a través de la Red, en relación tanto de la identidad del sujeto como del contenido de los datos, puede ser resuelto mediante la utilización de la firma electrónica digital. ¿El usuario que intenta acceder es quien dice ser?

Trazabilidad: Se corresponde con la creación, incorporación y conservación de información sobre el movimiento y uso de la información. Tener en cuenta la trazabilidad consiste en preocuparse sobre el propio ciclo de vida de la información, sobre la huella de sus acciones. ¿Se sabe en todo momento quién, cómo, cuándo y desde dónde accede a la información?

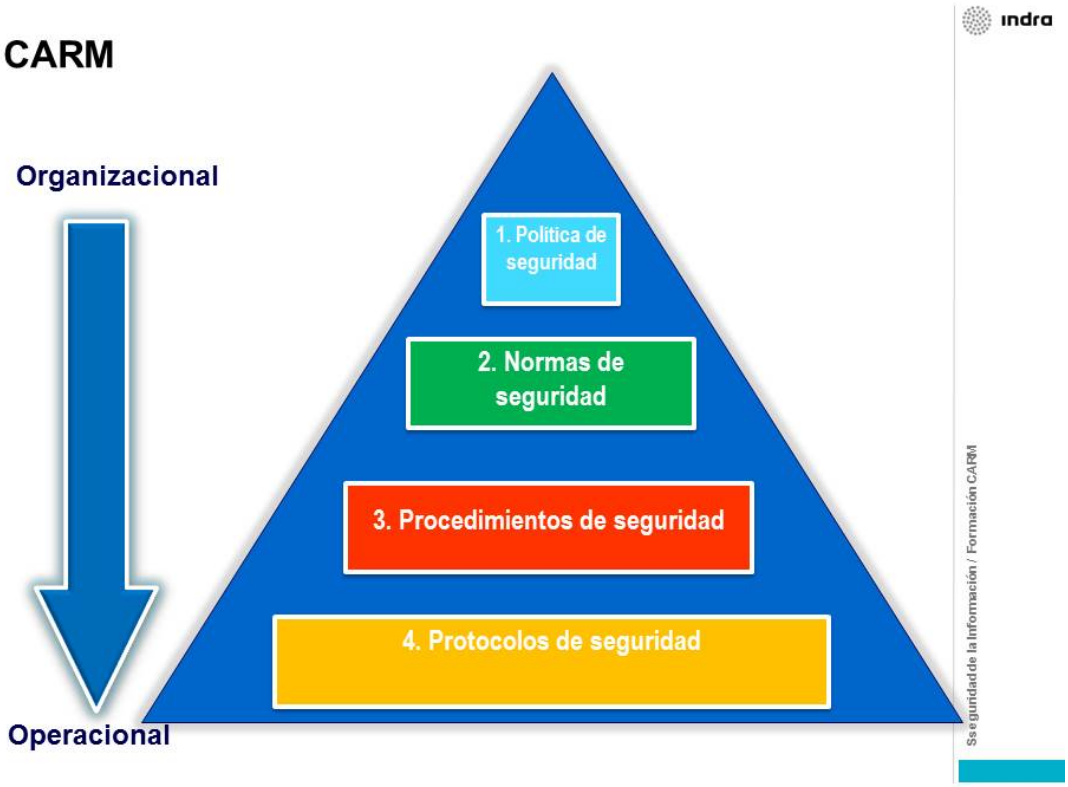
El cuerpo normativo sobre seguridad de la información se desarrolla en niveles por ámbito de aplicación, detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Esta jerarquía de documentos debe ser conexa y coherente para dar cumplimiento a las medidas de seguridad establecidas por el Real Decreto 3/2010. La Dirección General de Patrimonio, Informática y Telecomunicaciones desarrollan su marco normativo en base a los siguientes tipos de documento:

a) La Política de Seguridad de la Información que establece los requisitos y criterios de protección en el ámbito de la CARM.

b) Las Normas de Seguridad definirán qué hay que proteger y los requisitos de seguridad deseados correlacionado con la política de seguridad. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de la organización y deben también dar cumplimiento a la medida org.2 Normas de seguridad del R.D. 3/2010.

c) Los Procedimientos de Seguridad en los que describirá de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Son documentos que especifican cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos. Dará cumplimiento a la medida org.3 Procedimientos de seguridad del R.D. 3/2010.

Este conjunto de documentación podría verse esquematizada como se muestra en el siguiente gráfico;



La cantidad de documentación suele mayor conforme profundizamos en la base de la pirámide, con esto queremos expresar que normalmente el número de políticas de seguridad será menor que las normas de seguridad implantadas y a su vez el número de normas puede tener relacionados uno o más procedimientos de seguridad y para finalizar un procedimiento de seguridad puede llevar relacionados uno o más protocolos de seguridad asociados.

Del mismo modo conforme profundizamos en la pirámide se puede observar el recurso humano al que tiene asociado como destinatario, así por ejemplo, la política de seguridad es de ámbito organizacional y aplicaría a toda la organización, sin embargo, un procedimiento de seguridad podría ser de ámbito departamental, aplicando solo a un grupo reducido de personas, siempre teniendo en cuenta el nivel superior, en este caso, normas de seguridad y política de seguridad aplicables.

Esta jerarquía de tres niveles de documentación viene establecida como medidas de seguridad con carácter general que deben ser puestas en marcha para el cumplimiento del R.D. 3/2010. Además, pueden considerarse dos tipos más de documentos:

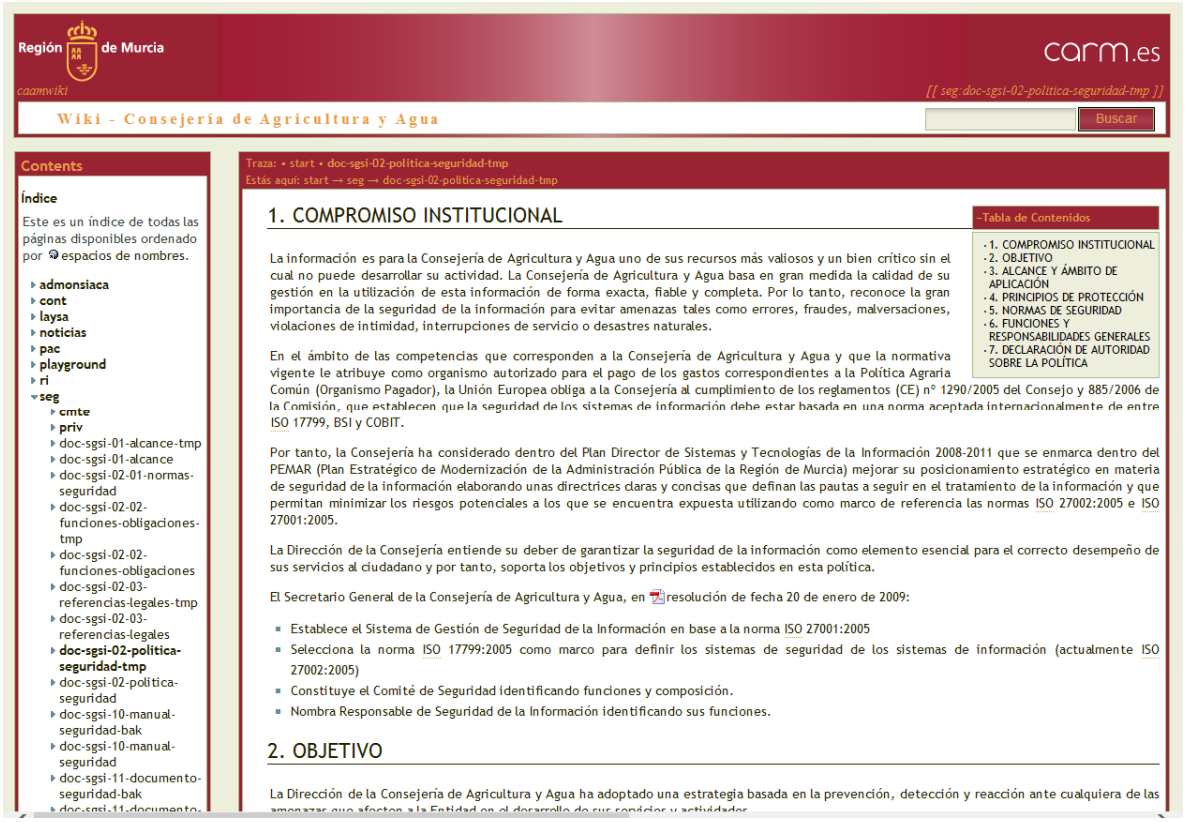
a) Basándose en los procedimientos de seguridad, y para entornos o sistemas de información concretos, podrán elaborarse instrucciones técnicas de seguridad que documenten de forma explícita y detallada las acciones técnicas a realizar en la ejecución del procedimiento o las tareas a considerar cuando se ejecute un procedimiento.

b) También podrán existir, como desarrollo de la propia política de seguridad o de cualquiera de las normas existentes, las normas de uso que establecen las reglas de comportamiento que deben cumplir los usuarios en el uso de los sistemas de información. Estos documentos destinados a usuario final resumirán y trasladarán los requisitos de seguridad a contemplar en la utilización o uso de determinadas tecnologías o servicios de manera concisa y fácilmente comprensible, así como lo que se considerará uso indebido y la responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente. Conforme a la disposición adicional novena del Decreto 302/2011, de 25 de noviembre, de Régimen Jurídico de la Gestión Electrónica de la Administración Pública de la Comunidad Autónoma de la Región de Murcia, las Consejerías competentes en materia de innovación de los servicios públicos y las competentes en materia de planificación informática y aplicaciones informáticas corporativas, aprobarán, mediante orden un Manual de Comportamiento en el uso de medios electrónicos para el personal de la Función Pública Regional.

En la URL, http://rica.carm.es se puede consultar varios enlaces y acceso a intranets de consejerías donde se puede consultar información relacionada con las políticas, normativas, procedimientos y protocolos de seguridad. Así por ejemplo se dispone de un "Área de seguridad", donde se puede consultar las Políticas de Seguridad vigentes y alguna información de ayuda al usuario.

Información relacionada con el uso del correo electrónico http://rica.carm.es/chacp/ecorreo_u/

En la intranet de la consejería de Agricultura y Agua disponen de un Sistema de Gestión de la Seguridad Informática (Norma ISO 27000), donde tienen declaradas por obligación de la norma una política de seguridad, normas de seguridad, procedimientos…etc. Se puede consultar en la siguiente URL → http://baseagri.carm.es/dokuwiki/doku.php



3. Políticas de seguridad. Herramienta organizacional

La misión de una política de seguridad es gestionar adecuadamente la protección de la información, los sistemas informáticos y el entorno tecnológico de la Comunidad Autónoma de la Región de Murcia, en adelante CARM, frente las amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

Las políticas son declaraciones de alto nivel[1] de la intención, las expectativas y la dirección de la gerencia. En una organización madura, las políticas pueden permanecer bastante estáticas debido a que son un conjunto de intenciones estratégicas de la organización, que no cambia con tanta asiduidad.

Un ejemplo de una declaración de política sobre el control de acceso puede ser la siguiente:

Los recursos de información deberán controlarse de un modo que restrinja efectivamente el acceso no autorizado.

Como puede observarse la declaración es muy genérica sin entrar en profundidad.

Las políticas pueden considerarse como la "constitución" del gobierno de la seguridad de la información y deben estar claramente alineadas con los objetivos estratégicos de la seguridad de la organización.

A continuación vamos a exponer los siguientes conceptos que no deberían faltar en una Política de Seguridad;

- Principios de protección de la información
- Seguridad como proceso continuo y preventivo
- Análisis y gestión del riesgo
- Seguridad por defecto desde el diseño hasta la implementación
- Garantías de terceros y externos
- Protección de datos de carácter personal
- Clasificación de la información
- Gestión de la seguridad y mejora continua
- Control de acceso lógico.

[1] Un documento de alto nivel no entra en detalles técnicos. Los documentos de alto nivel suelen sufrir menos modificaciones que los documentos operacionales o de bajo nivel.

- Organización de la seguridad.
- Responsabilidades del personal
- Uso adecuado de los recursos informáticos del puesto de trabajo
- Protección de infraestructuras físicas

Principios de protección de la información

Toda política de seguridad se basará en unos principios básicos de protección que forman los pilares sobre los que se sustentan y sustentarán todas las actuaciones en materia de seguridad de la información que realice la CARM, estos principios básicos son:

- Seguridad integral. La seguridad es un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema.

- Gestión de riesgos. La gestión de los riesgos que pudieran afectar a la información debe estar en continua revisión para detectar posibles nuevas amenazas.

- Prevención, reacción y recuperación. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen.

- Líneas de defensa. Los sistemas han de disponer de una estrategia de protección constituida por múltiples capas de seguridad. Con este principio se pretende evitar la focalización de todos los esfuerzos en seguridad sobre un solo frente, de manera que si consiguen burlar este perímetro estaría todo el sistema expuesto.

- Reevaluación periódica. La evolución de las amenazas obliga a un análisis continuo de posibles fallos en la seguridad de la información de los sistemas.

  "Si tu sistema es seguro es que no lo ha atacado la persona adecuada."

- Función diferenciada. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

Seguridad como proceso continuo y preventivo

La seguridad de la información debe entenderse como un proceso continuo de vigilancia y mejora que engloba a todos y cada uno de los elementos humanos, técnicos, materiales y organizativos que participan de forma directa o indirecta en el día a día de los usuarios de la CARM.

El objetivo básico de todas las actuaciones en materia de seguridad de la información será evitar la ocurrencia de incidentes o al menos minimizar su impacto cuando estos sucedan.

Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición a los riesgos que tengan mayores consecuencias para la CARM.

Se incorporarán también medidas de detección temprana de incidentes que estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se resuelvan en la mayor brevedad de tiempo posible.

En cualquier caso, también se dispondrá de medidas de recuperación que permitan la restauración de la información y los servicios en aquellos casos donde las medidas de seguridad no se muestren eficaces para paliar las amenazas previstas de forma que se pueda hacer frente a eventos o sucesos imprevistos sin producir mermas significativas en la CARM.

Análisis y gestión del riesgo

Dado que los sistemas de información son entornos cambiantes y la naturaleza de las amenazas también es dinámica, las decisiones en materia de seguridad deben basarse en el análisis y gestión de riesgos como proceso esencial de seguridad, que deberá mantenerse permanentemente actualizado. La evaluación de riesgos identifica las amenazas y vulnerabilidades y debe ser suficientemente amplia para abarcar los principales factores internos y externos tales como factores tecnológicos, físicos y humanos, políticos y servicios de terceros con implicaciones de seguridad.

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad a aplicar.

Debido a la creciente interconexión de los sistemas de información, la evaluación de riesgos debe incluir la consideración de los posibles daños que pueden proceder de agentes externos o ser causados por terceras personas.

Seguridad por defecto desde el diseño hasta la implementación

Los sistemas de información deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. La incorporación de las medidas de seguridad deberá tenerse en cuenta durante el diseño, adquisición, construcción, contratación, explotación de los sistemas de información que dan soporte a los servicios de la CARM.

Garantías de terceros y externos

En la construcción, diseño o mantenimiento de los sistemas de información que dan soporte a la CARM pueden participar empresas o terceros que suministran servicios o productos. Con el objetivo de garantizar la coherencia y cohesión de las medidas de seguridad, cualquier empresa o tercero que suministre productos o servicios deberá garantizar el cumplimiento de las medidas de seguridad requeridas por la política de seguridad de la CARM.

La contratación de servicios o productos vinculados a la CARM deberán incorporar cláusulas de acuerdos de nivel de servicio donde se determinen los requisitos mínimos de seguridad a

garantizar así como los procedimientos de notificación y gestión de incidentes a utilizar si el prestador sufriera un incidente de seguridad que pudiera afectar a la CARM. Estas entidades deberán nombrar un responsable de seguridad que actúe como interlocutor válido a los efectos de la coordinación en esa materia.

Protección de datos de carácter personal

La seguridad de los sistemas de información debe ser compatible con los valores esenciales de una sociedad democrática, tratando de preservar y proteger dichos valores respecto de los datos que sean custodiados por la CARM en relación a los servicios que presta. La presente política de seguridad de la información deberá garantizar el cumplimiento de los diferentes documentos de seguridad exigidos por el Real Decreto 1720/2007 y satisfacer un nivel de protección adecuado para los datos de carácter personal que sean tratados los sistemas de información que dan soporte al ejercicio de los derechos y el cumplimiento de deberes a través de medios electrónicos en cumplimiento de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

Clasificación de la información

Toda la información tratada deberá ser clasificada atendiendo al tipo de información y su naturaleza de acuerdo con los criterios establecidos por los artículos 80 y 81 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.

Toda la información tratada en la CARM deberá tener asignado un responsable de información que será quien determine el nivel de protección a asignar por parte de la unidad competente por razón de la materia. Esta clasificación de información será válida tanto para el soporte electrónico como la información en soporte papel.

El nivel de protección y las medidas de seguridad a aplicar será proporcional al resultado de dicha clasificación (principio de proporcionalidad), atendiendo a los criterios mínimos establecidos al menos por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y los criterios establecidos el 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.

Gestión de la seguridad y mejora continua

La gestión de la seguridad de la información requiere una evaluación y una auditoría continua para comprobar que los requisitos establecidos por el R.D. 3/2010 se cumplen y que las medidas de seguridad son eficaces proporcionando el nivel de seguridad deseado.

Los planes para la mejora de la seguridad de la información contendrán una descripción de las líneas de actuación previstas, proyectos, indicadores de cumplimiento y de progreso, así como métricas para evaluar la efectividad. Estos planes se revisarán anualmente teniendo en cuenta los resultados de las auditorías y de las evaluaciones de riesgos. Los planes estratégicos, los informes de seguimiento y las revisiones anuales se someterán a la aprobación de los

responsables de la información o de los responsables de tratamiento, según corresponda. Al menos de forma bienal, los sistemas de información de la CARM serán auditados para supervisar explícitamente el nivel de cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración y el 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 y establecer las medidas correctoras necesarias para solventar las deficiencias detectadas por la auditoría. El informe de auditoría será presentado por el Responsable de Seguridad al Comité de Seguridad del organismo auditado.

Asimismo la gestión de la seguridad implica llevar un control de los incidentes de seguridad que se hayan producido de forma que puedan ser valorados y permitan introducir los cambios necesarios para que no se vuelvan a producir, generando las correspondientes acciones preventivas, correctivas o de mejora que sean necesarias tras analizar los hechos. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

Control de acceso lógico.

El acceso a los recursos informáticos del puesto de trabajo y las aplicaciones que forman los sistemas de información de la CARM se realizará siempre de forma controlada, garantizando la adecuada identificación del usuario de forma que permita conocer qué persona realiza el acceso. Por tanto, los identificadores de usuario entregados al personal serán únicos e intransferibles. También podrán utilizarse otros medios de autenticación más robustos que empleen el uso de biometría o de certificados digitales según establezca la política de firma electrónica de la Administración Regional. Los sistemas de información deberán contemplar los mecanismos de registro y auditoría de accesos necesarios que permitan conocer en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

Organización de la seguridad.

La Consejería de Economía y Hacienda regulará mediante orden la estructura organizativa que dé soporte a la presente política de seguridad de la información. Para ello y en cumplimiento del Art. 10 del R.D. 3/2010 se establecerán unos roles corporativos que ostenten con carácter general las figuras de responsable de información, responsable de servicio, responsable de seguridad y responsable de sistemas de información. Todos estos nombramientos formarán el Comité de Seguridad corporativa de la Administración Regional.

De la misma forma, se definirán las funciones y responsabilidades de las figuras de responsable de información, responsable de servicio, responsable de seguridad cuyo ámbito de actuación se circunscriba a las Consejerías, organismos públicos y entidades de derecho público que presten servicios a través de la Sede electrónica de la Administración Regional. Todos estos nombramientos en estos organismos formarán el Comité de Seguridad en las Consejerías, organismos públicos y entidades de derecho público.

La figura de responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Para garantizar la segregación de funciones, se añadirá la figura de responsable de sistemas de información que velará por la disponibilidad y funcionamiento del entorno tecnológico que da soporte a la prestación de los servicios de Administración Regional.

En la citada orden se regularán las atribuciones de cada responsable y los mecanismos de nombramiento, coordinación y resolución de conflictos.

La Administración Regional habilitará los medios técnicos necesarios para facilitar esa coordinación. Los responsables de seguridad actuarán de manera coordinada en la aplicación y control de las medidas de seguridad

Responsabilidades del personal

La política de seguridad tiene carácter obligatorio para todo el personal al servicio de la CARM, especialmente para quienes participen en el tratamiento de información o tengan acceso a los locales donde se custodie la información o se realice su tratamiento independientemente del tipo de relación jurídica o laboral que se mantenga con la CARM.

Todo el personal al servicio de la CARM debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, así como que ellos mismos son una pieza esencial para el mantenimiento y mejora de la misma. El conocimiento de los riesgos es la primera línea de defensa para la seguridad de los sistemas de información. Para mitigarlos, la Dirección General de Patrimonio, Informática y Telecomunicaciones desarrollará un marco normativo en materia de seguridad corporativa y el conocimiento y cumplimiento de dichas normativas de seguridad contribuirán de modo efectivo a reducir los potenciales riesgos que pudieran afectar al buen funcionamiento de los sistemas de información. Es por ello que el personal al servicio de la CARM deberá estar debidamente concienciado sobre esta materia para que pueda ser capaz de detectar posibles incidentes que pudieran perjudicar seriamente los sistemas de información.

El incumplimiento de la política de seguridad podrá tener consecuencias disciplinarias, de acuerdo con el régimen sancionador aplicable en cada caso, sin perjuicio de otras responsabilidades en que se pudiera incurrir.

Uso adecuado de los recursos informáticos del puesto de trabajo

La CARM proporciona equipamiento informático en los puestos de trabajo según las necesidades para el desempeño de las funciones encomendadas. Dichos equipos no están destinados al uso personal. Este equipamiento no podrá utilizarse para actividades ilícitas o irregulares, o que afecten negativamente al funcionamiento de la CARM o sean contrarias a los intereses de ésta.

La instalación o utilización de elementos hardware o software ajenos a los que forman parte de la configuración del puesto de trabajo requerirán una autorización previa por parte del órgano competente en materia de tecnologías de la información que corresponda.

Protección de infraestructuras físicas

Las infraestructuras informáticas y de comunicaciones que no formen parte de los puestos de trabajo distribuidas por los diferentes edificios de la Administración Regional deberán ubicarse en áreas separadas, de acceso restringido y suficientemente protegidas de acuerdo con la naturaleza de la información y de los servicios en que intervengan.

Los centros de procesos de datos donde se alberguen los sistemas de información que dan soporte a servicios de Administración Regional deberán ubicarse en edificios especialmente acondicionados a tal efecto. Deberán contar con medidas de control medioambiental, control de visitas y accesos así como un servicio de monitorización 24x7x365 días que supervise el correcto funcionamiento de las instalaciones y los servicios que desde éstas se proporcionan.

4. Normas de seguridad. Herramienta de gestión

Las normas son las mediciones, los límites permisibles o los procesos usados para determinar si los procedimientos, procesos o sistemas cumplen con los requerimientos en la política.

Por lo general, una norma debe establecer parámetros suficientes para determinar sin ambigüedad que un procedimiento o práctica cumple con los requerimientos de la política en cuestión.

A continuación vamos a ver una normativa de la CARM denominada "*Manual de comportamiento en el uso de medios electrónicos para el personal de la Función Pública Regional"* que tiene por objeto establecer las normas de seguridad que deben aplicarse en el puesto de trabajo por parte de los empleados públicos de la administración regional, con la finalidad de hacer efectivos los principios de protección de la información establecidos en ella.

Es importante considerar que los medios electrónicos y recursos informáticos de los que hace uso el empleado público están dentro del alcance de aplicación del manual de comportamiento. Son medios electrónicos y recursos TIC de la Administración Regional todos los sistemas de información centrales y ubicados en Consejerías u otros organismos, servidores y estaciones de trabajo, ordenadores de puesto de trabajo, equipos portátiles, teléfonos de última generación (Smartphones) y tabletas electrónicas, impresoras y otros periféricos y dispositivos de salida de datos, sistemas de localización, redes internas y externas, sistemas multiusuario y servicios de comunicaciones (transmisión telemática de voz, imagen, datos o documentos) y almacenamiento que sean de su propiedad, así como las aplicaciones informáticas (software) que estén alojadas en cualquiera de los sistemas o infraestructuras referidos.

En este ámbito no se considera un "recurso TIC de la Administración Regional" aquellos ordenadores personales financiados a título individual, no inventariados a nombre de Administración, aunque pudieran ocasionalmente ser usados para labores propias del personal de la Administración Regional. En estos casos, la Administración Regional se reserva el derecho de proporcionar acceso a la red corporativa desde este tipo de recursos ajenos a la misma si se producen uno o ambos de los siguientes casos;

- no se proporcionan unos mínimos requisitos de seguridad;
    - Conocimiento y aplicación por parte del usuario de las normas de uso de la CARM.
    - Tener un software antivirus instalado y actualizado (módulos del programa y base de datos de firmas.
    - No tener instalado software ilegal, sin licencia o no permitido por esta norma de seguridad de la CARM a no ser que esté validado por el responsable competente.

- Disponer de cortafuegos en el equipo.
- Tener actualizado el sistema operativo con los últimos parches de seguridad.
- Tener configurado el equipo con un usuario y una contraseña.

- existen indicios o evidencias de un incidente potencial de seguridad que pueda comprometer o bien la seguridad de la información de los recursos TI de la Administración Regional o bien su buen nombre o imagen corporativa.

En caso de ser autorizados, estos recursos deberán cumplir con las medidas de seguridad que técnicamente les apliquen del Manual de Comportamiento.

La norma de seguridad consta de los apartados que se detallan a continuación;

Contenidos inapropiados e ilícitos

Se consideran contenidos inapropiados e ilícitos los elementos que sean susceptibles de atentar o que induzcan a atentar contra la dignidad humana, la seguridad y los derechos de protección de las personas menores de edad y, especialmente, en relación con los siguientes:

a) Los contenidos que atenten contra el honor, la intimidad y el secreto de las comunicaciones de las personas con especial atención a preservar los derechos de los menores de edad para rechazar su utilización, especialmente con objetivos sexuales, y para mantener una actitud de cautela en la difusión de contenidos potencialmente nocivos para la infancia.

b) Los contenidos violentos, degradantes o favorecedores de la corrupción de menores, así como los relativos a la prostitución o la pornografía de personas.

c) Los contenidos que pretendan alterar el orden público, de forma que la Red corporativa de telecomunicaciones de la CARM sea empleada como vehículo de mensajes que inciten al uso de la violencia o a la participación en actividades delictivas.

d) Los contenidos que den soporte a la comisión de delitos económicos o vinculados con la estafa a consumidores, velando por respetar los principios de transparencia y sometiéndose a las normativas de protección del consumidor.

e) Los contenidos racistas, xenófobos, sexistas, los que promuevan sectas y los que hagan apología del crimen, del terrorismo o de ideas totalitarias o extremistas.

f) Los contenidos que fomenten la ludopatía y consumos abusivos de sustancias estupefacientes fuera del ámbito sanitario.

g) Los contenidos de sitios que ofrecen o promueven la colección de información sin conocimiento y sin consentimiento explícito del usuario final.

h) Los contenidos que albergan comunidades de usuarios donde interactúan, publican mensajes, fotos y se comunican entre ellos, siendo focos de gran difusión de infección

de equipos y ataques mediante ingeniería social o suplantación de identidad para la obtención de información confidencial.

i) Los contenidos que proporcionen métodos para obtener acceso a direcciones URL eludiendo las medidas de seguridad establecidas.

j) Los contenidos que faciliten o alberguen grandes salidas de información quedando al descubierto la pérdida de control sin que se garanticen unas medidas de seguridad que determinen, la responsabilidad final de los datos, la confidencialidad e incluso el derecho a la propiedad intelectual de los mismos

Usos inadecuados e ilícitos.

Se considera un mal uso o uso inaceptable a aquella actuación del usuario que puede afectar a la disponibilidad de un servicio, al trabajo del resto de usuarios, a la confidencialidad y seguridad de la información o que, en general, ponga en riesgo cualquiera de las cinco dimensiones de seguridad (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) de la información y los servicios.

La siguiente lista, aunque no es exhaustiva y no incluye todos los casos, constituye un conjunto de ejemplos de lo que se consideran malos usos:

a) Cualquier actividad que vulnere el derecho fundamental a la intimidad de las personas según lo tipificado en el Art. 197 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal vinculado al descubrimiento y revelación de secretos.

b) El uso de una cuenta de usuario para la que no se tiene autorización (suplantación de identidad) o bien el robo de credenciales (usuario y contraseña).

c) El uso de la Red corporativa de la CARM para conseguir el acceso no autorizado a cualquier ordenador, servidor o aplicación, ya sea de la propia Administración Regional o de cualquier otra Organización que vulnere el Art. 197 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

d) Realizar alguna actuación de forma intencionada que interfiera en el funcionamiento normal de otros ordenadores, impresoras, dispositivos o redes.

e) Provocar la congestión de los enlaces de comunicaciones o sistemas informáticos.

f) Intentar o lograr la destrucción o modificación premeditada de la información de otros usuarios.

g) Instalar y ejecutar de forma intencionada en cualquier ordenador o subred cualquier tipo de software que provoque el mal funcionamiento o la sobrecarga en dicho equipo o subred (malware). También se incluye aquí la cesión de este malware a otros usuarios.

h) El abuso deliberado de los recursos puestos a disposición del usuario.

i) Los intentos de saltarse medidas de protección de la información o de explotar posibles fallos de seguridad de los sistemas.

j) El no cumplimiento de las condiciones de las licencias del software o de sus derechos de autor.

k) El envío de mensajes de correo con contenido fraudulento, injurioso, amenazante o presumiblemente constitutivo de delito.

l) Ocultar o falsificar la identidad de una cuenta de usuario o de una máquina.

m) El uso de los servicios de difusión de información para fines que no tengan relación con las propias del desempeño laboral o que suponga una violación de las restricciones de secreto o confidencialidad asignadas a la información difundida.

n) Los intentos de monitorización y rastreo de las comunicaciones de los usuarios.

Mecanismos de seguridad y protección de la red corporativa.

Tecnologías de prevención de incidentes y detección de anomalías.

La Administración Regional velará para que las medidas de prevención y seguridad en el uso de los medios electrónicos e Internet por parte del personal de la Administración Regional garanticen el cumplimiento de los principios de protección establecidos por la política de seguridad de la información aprobada. Para ello, seleccionará, implantará y gestionará aquellas medidas de seguridad que considere más eficaces para garantizar el cumplimiento de los principios de seguridad habida cuenta del estado de la tecnología y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

La Administración Regional se reserva el derecho de auditar toda actividad realizada en sus sistemas.

Sistemas de control de las conexiones

La Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas establecerá unas reglas de uso de los protocolos de Internet que definan los servicios autorizados con carácter general dentro de la red de datos corporativa así como los servicios pre-autorizados desde Internet hacia la red corporativa y los servicios que conectan desde la red corporativa hacia Internet.

El sistema de control de conexiones (firewall) puesto a disposición por la Dirección General competente en materia de TIC se sujetará a los siguientes criterios de configuración:

a) Estará basado en el principio de mínimos privilegios, por lo que se autorizarán siempre los protocolos de comunicaciones estrictamente necesarios que permitan suministrar los servicios requeridos.

b) Ofrecerá información a los responsables técnicos de las distintas Consejerías usuarias de la Red corporativa sobre los procedimientos de supervisión y los criterios de los mismos.

c) Estudiar qué otras consideraciones realizar.

Sistemas de Filtrado.

La Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas supervisará de forma proactiva el adecuado uso de Internet y la Red corporativa de telecomunicaciones contemplando para ello el uso efectivo de sistemas de filtrado, que bloqueen o discriminen contenidos o usos inapropiados según lo regulado en los apartados Contenidos inapropiados e ilícitos y Usos inadecuados e ilícitos del presente texto.

El sistema de filtrado puesto a disposición por la Dirección General competente en materia de TIC se sujetará a los siguientes criterios de configuración:

a) Aportará información a los usuarios sobre los valores, criterios y métodos de filtrado que se utilizan.

b) Ofrecerá información a las personas usuarias sobre los procedimientos de supervisión y los criterios establecidos.

La Consejería competente en materia de TIC comprobará periódicamente la efectividad de estas herramientas e incorporará aquellos otros instrumentos que la tecnología desarrolle.

Criterios generales de filtrado de contenidos.

La Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas formalizará la política de filtrado de contenidos mediante un documento escrito donde detallarán las distintas categorías a gestionar y el criterio o decisión de filtrado a aplicar. Para aquellas categorías que sean propuestas como "prohibidas o filtradas" deberá aportar información sobre los motivos por los que dicha decisión ha sido tomada. Para ello, podrán argumentarse en base los siguientes criterios:

a) Criterios de seguridad de la información, justificando los riesgos por los que se considera no adecuado el tráfico de dichos contenidos.

b) Criterios organizativos internos, justificando por qué dichos contenidos no son considerados adecuados dentro de la red corporativa a atendiendo a valoraciones sobre cómo impactan en la productividad laboral, la imagen de la Administración Regional ante los medios de comunicación, etc…

Esta política de filtrado de contenidos será revisada al menos con una periodicidad anual y deberá valorar las quejas o sugerencias realizadas por los diferentes organismos sometidos a dicha política de filtrado. La valoración final y aprobación de la política de filtrado de contenidos revisada deberá ser aprobada por el Comité de Seguridad de la Información según establece la Política de Seguridad de la Información de la Administración Regional.

Excepciones a los criterios de filtrado de contenidos y autorizaciones necesarias.

La Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas podrá autorizar excepciones a los criterios de filtrado anteriores siempre que un usuario requiera acceder por razones vinculadas al desempeño de su trabajo a una categoría bloqueada.

Para eludir dicho filtrado de contenidos, el usuario que requiera acceso debe dirigirse al Responsable de Personal de su Consejería u Organismo Autónomo, para que, en su caso, tramite la oportuna petición de autorización que se formalizará dentro de los diferentes servicios gestionados por la Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas.

Si se automatizara este procedimiento, se realizaría por parte del usuario una petición de catálogo a la Dirección General competente en materia de planificación informática, sistemas

de información y aplicaciones informáticas corporativas, debiendo adjuntar el documento de autorización firmado por Secretario General de la Consejería o equivalente en el Organismo.

En el documento a firmar y en la petición constarán los riesgos asociados a todas las categorías filtradas, y la instrucción de que el usuarios debe autenticarse diariamente de forma previa a la navegación restringida y que todo tráfico excepcional será registrado e identificado en nuestros sistemas perimetrales

Errores en el sistema de calificación de contenidos y solicitud de ajustes

Cuando cualquier usuario de la Red corporativa de telecomunicaciones detecte la existencia de un posible error en la catalogación o una asignación incorrecta de categorías, se notificará la dirección electrónica como incidente a la Dirección General competente en materia de planificación informática y aplicaciones informáticas corporativas para que ésta lo comunique al fabricante del producto software de filtrado de conexiones para que valore de nuevo dicha categoría. También se realizará dicha solicitud si por parte del personal técnico de la Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas hay indicios de que la categoría está mal asignada. Si el fabricante del producto software ratifica el criterio empleado y no modifica la categoría inicial asignada, se informará al usuario de la posibilidad de solicitar una autorización individual por razones vinculadas al desempeño de su trabajo a la categoría bloqueada, procedimiento contemplado en el aparatado Excepciones a los criterios de filtrado de contenidos y autorizaciones necesarias.

Protección de datos de carácter personal

La Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas garantizará el cumplimiento de la legislación en materia de protección de datos de carácter personal durante cualquiera de las fases de tratamiento de información perteneciente al sistema de filtrado de contenidos y control de conexiones así como a la legislación existente en materia de protección del secreto de las telecomunicaciones.

Usos de medios electrónicos regulados

Acceso y conexión de la red de telecomunicaciones corporativa de la CARM

La Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas es la responsable de la administración y gestión de la red corporativa de comunicaciones de la CARM. Para ello, deberán satisfacerse los siguientes requisitos:

a) La instalación de nuevos puntos de red conectados a la Red corporativa de telecomunicaciones se hará de conformidad con los criterios aprobados y será competencia exclusiva de la Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas.

b) No se permitirá la instalación de electrónica de red y de puntos de acceso de redes inalámbricas con conexión a la Red corporativa de telecomunicaciones de la CARM sin la debida información y autorización de la Unidad de Informática. En caso de detección de algún equipo no autorizado se procederá a su inmediata desconexión.

c) Los equipos electrónicos de gestión e infraestructura de la Red corporativa de telecomunicaciones de la CARM serán instalados, configurados y mantenidos exclusivamente por la Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas.

d) Todos los equipos que se conectan a la red deben recibir una dirección IP y un nombre de red asignados por el direccionamiento interno de la Red corporativa de telecomunicaciones de la CARM, además de ser incluidos en el registro correspondiente.

NOTA: Un problema de seguridad en cualquiera de las máquinas internas del perímetro podría afectar colateralmente a la seguridad del resto. Por tanto, se podrían establecer unos mínimos para que un servidor tenga una IP dentro de la Red corporativa

Uso de la red de telecomunicaciones corporativa de la CARM

La Dirección General competente en materia de planificación informática, sistemas de información y aplicaciones informáticas corporativas es la responsable de la monitorización y vigilancia del correcto uso de la red corporativa de comunicaciones de la CARM. Para ello, deberán satisfacerse los siguientes requisitos:

a) No se permite el empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar a la topología o a la estructura lógica de la red.

b) Los usuarios de la red no deben utilizar esta infraestructura y servicios para otros usos que no sean los permitidos en el presente manual de comportamiento de uso de

medios electrónicos o los propios necesarios para el desempeño de su actividad profesional.

c) Se deben habilitar mecanismos seguros (protocolos seguros, VPNs) para conexiones externas a nuestra red que requieran de unas condiciones de confidencialidad, integridad y autenticidad altas.

d) Ningún usuario está autorizado a utilizar analizadores del tráfico que circula por la red corporativa de comunicaciones de la CARM. Igualmente está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido a los administradores de la red y bajo situaciones especiales (incidentes de seguridad, denuncias de usuarios, etc.) que lo justifiquen.

e) Queda prohibido el uso de mecanismos VPN no autorizados a rede públicas o privadas no autorizadas.

f) En el caso de entornos con terminales externos (de cara al público) será necesario utilizar técnicas de securización suplementarias (BYOD, NAC).

Responsabilidades de los usuarios en el uso de medios electrónicos.

Uso del puesto de trabajo en el entorno laboral

Los equipos personales de trabajo, físicos o virtuales, y los dispositivos informáticos son recursos tecnológicos proporcionados por la Administración Regional para permitir el desempeño de las funciones y responsabilidades del personal.

El uso de equipos o dispositivos no administrativos deberá ser aprobado previamente por el Servicio de Gestión Informática del organismo del usuario.

En ambos casos se solicita que el personal de la Función Pública Regional dé cumplimiento a las siguientes normas de seguridad, para lo cual podrá ser asistido por su Servicio de Gestión Informática:

- Emplear los sistemas de información únicamente para fines propios de su trabajo, siempre respetando la política de seguridad de la Administración Regional.
- Utilizar contraseñas fuertes en todos los servicios, para dificultar la suplantación de identidad (evitar nombres, fechas, datos conocidos o deducibles, palabras del diccionario, etc.). Las condiciones impuestas a la hora de establecer la contraseña o cambiar la actual, son las siguientes;
    - Ser distinta de las últimas 10 empleadas.
    - Tener al menos 8 caracteres.
    - Contener al menos una mayúscula, una minúscula y un número.
    - No contener (ni en mayúsculas ni minúsculas ni combinación de ambas): login, nombre, primer apellido, segundo apellido, teléfono, mail, carm, password, 1234, qwerty, ni dos caracteres iguales en posiciones consecutivas (aa, 11...).

  Recuerde que debe tener en cuenta lo siguiente;

    - Custodiar todo identificador, contraseña o mecanismos de firma electrónica utilizado para el acceso a o la utilización de los sistemas de la información de la Administración Regional, guardando la debida diligencia para impedir el acceso o conocimiento por otras personas.
    - Comunicar a su Servicio de Gestión Informática la pérdida, olvido o sospecha de conocimiento por otra persona.
    - Cambiar las contraseñas regularmente (al menos una vez al año) y siempre que haya cualquier indicación de posible compromiso en el sistema o en la contraseña.

- Mantener los sistemas de protección activos y actualizados, así como aplicar los parches de seguridad.
- Realizar copias de seguridad con cierta frecuencia para evitar la pérdida de datos importantes. Las copias de seguridad se realizarán siguiendo las instrucciones de su Servicio de Gestión Informática. Si requiere realizarla en dispositivos deberán ser previamente autorizadas.
- No instalar aplicaciones no autorizadas por su Servicio de Gestión Informática.
- Apagar el equipo cada vez que concluya la jornada laboral o durante una ausencia larga a no ser que se tengan instrucciones contrarias del Servicio de Gestión Informática.
- Bloquear el equipo en caso de ausentarse y utilizar salvapantallas con contraseña.
- Impedir el acceso no autorizado al material empleado.
- Solicitar autorización a su Servicio de Gestión Informática antes de introducir o sacar soportes de información de las dependencias administrativas. En este último caso, aplicar las medidas necesarias para que no sea accesible por personal no autorizado.
- Comunicar a su Servicio de Gestión Informática cualquier incidencia o evento que afecte a la seguridad de los sistemas de información.

Uso de claves y sistemas de firma electrónica

Se solicita que el personal de la Administración Regional dé cumplimiento a las siguientes normas de seguridad:

- Custodiar todo identificador, contraseña o mecanismos de firma electrónica utilizado para el acceso y/o la utilización de los sistemas de la información de la Administración Regional, guardando la debida diligencia para impedir el acceso o conocimiento por otras personas.
- Comunicar a su Servicio de Gestión Informática la pérdida, olvido o sospecha de conocimiento por otra persona.
- Cambiar las contraseñas regularmente (al menos una vez al año) y siempre que haya cualquier indicación de posible compromiso en el sistema o en la contraseña
- La firma electrónica asignada al personal al servicio de la Función Pública Regional será personal e intransferible.
- El personal es responsable de la custodia de la tarjeta inteligente donde se encuentra almacenada la firma electrónica.

Uso del correo electrónico corporativo

El correo electrónico corporativo es un medio de comunicación proporcionado por la Administración Regional para permitir el desempeño de las funciones y responsabilidades del personal. Por tanto, se solicita que el personal de la Función Pública Regional dé cumplimiento a las siguientes normas de seguridad:

- Emplear este medio de comunicación únicamente para fines propios de su trabajo, siempre respetando la política de seguridad de la Administración Regional.
- Atender a normas de buena conducta dado que representa en todo momento a la Administración Regional.
- No responder a correos en los que se pida datos confidenciales, como cualquiera de sus contraseñas.
- No abrir ni ejecutar ficheros, ni abrir enlaces, que se reciban por correo electrónico de desconocidos o que no se tenga prevista su recepción aunque sea de un conocido.
- No utilizar el correo electrónico para transmitir mensajes que puedan poner en peligro la confidencialidad.
- Enviar correos exclusivamente a las personas interesadas en el asunto del mismo.
- No facilitar la dirección de correo laboral propia ni de otros usuarios de la Administración en entornos no laborales. Evitar que correos enviados fuera de la Administración puedan incluir esta información en el contenido o en los campos "Para" o "CC" (Con Copia). Utilizar en su lugar el campo "CCO" (Con Copia Oculta).
- El correo electrónico no es un sistema de almacenamiento de información sino de intercambio y comunicación. Por tanto, los documentos y archivos necesarios para el trabajo deben guardarse en carpetas de trabajo, no en el buzón de correo.
- Eliminar periódicamente todos aquellos correos innecesarios o cuya información haya caducado y no sea útil. El buzón de correo tiene un tamaño limitado y por tanto, debe gestionar adecuadamente su uso.

Uso de Internet desde el puesto de trabajo

El acceso a Internet proporcionado por la Administración Regional al personal de la misma es una herramienta para permitir el desempeño de las funciones y responsabilidades del personal. Por tanto, se solicita que el personal de la Función Pública Regional dé cumplimiento a las siguientes normas de seguridad:

- El usuario cumplirá las medidas de seguridad implantadas en relación al filtrado de contenidos en la red corporativa de comunicaciones de la CARM.
- El usuario no intentará utilizar herramientas que eviten la aplicación de la política de filtrado de contenidos en la red corporativa de comunicaciones de la CARM.

Consecuencias del mal uso de los medios electrónicos

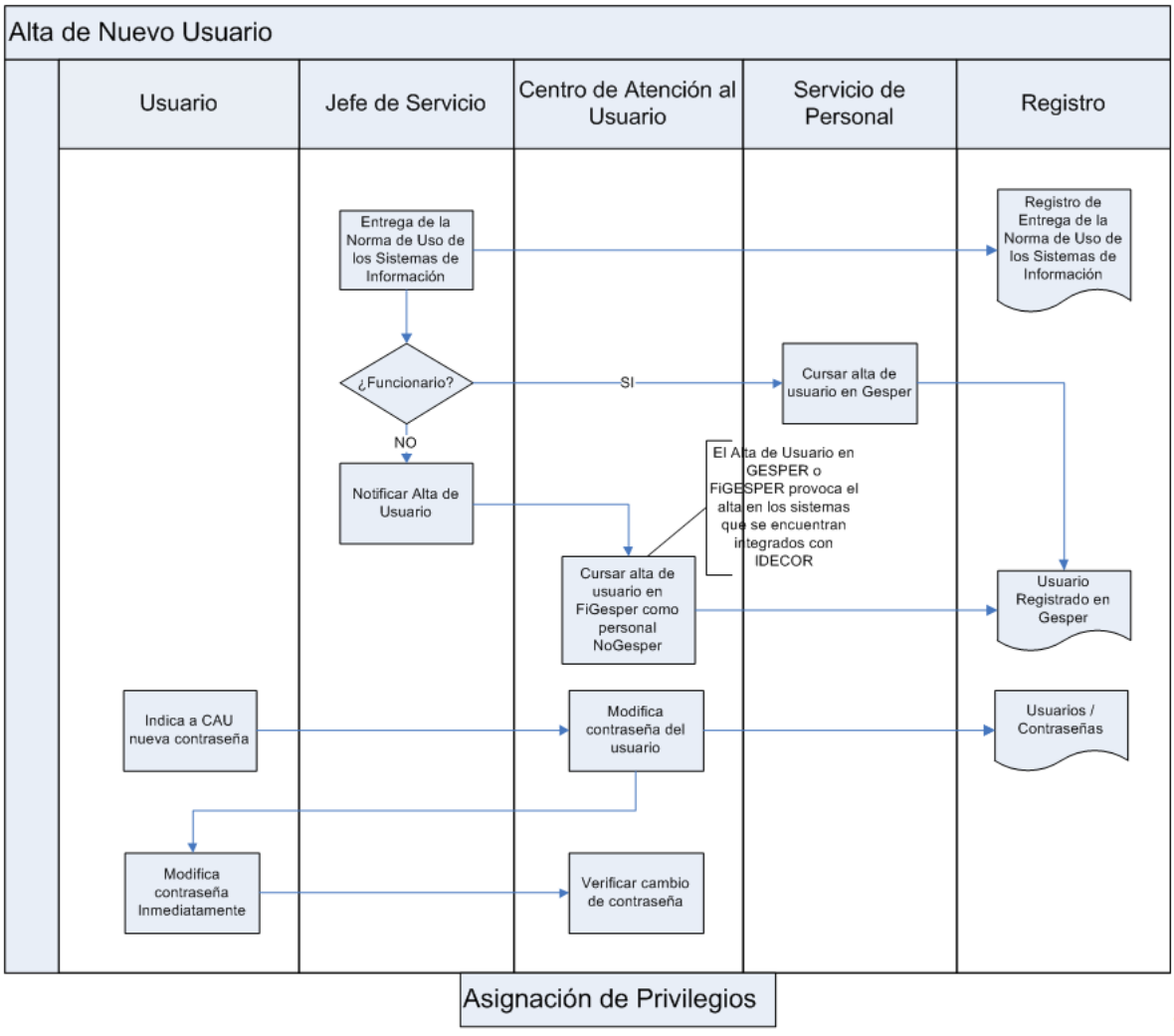
El incumplimiento de la presente normativa puede suponer el establecimiento de medidas disciplinarias, según se contemple en la legislación en vigor[2], así como encausamiento judicial en casos de acto premeditado con intención de provocar, o provocando, un perjuicio para la Administración Regional

[2] Decreto Legislativo 1/2001, de 26 de enero

5. Procedimientos de seguridad. Herramientas de operación

Los procedimientos son responsabilidades de operaciones, incluyendo operaciones de seguridad, pero se incluyen en este manual para brindar mayor claridad. Los procedimientos deben ser claros e incluir todos los pasos necesarios para cumplir con tareas específicas. Deben definir resultados y exposiciones esperados, así como las condiciones requeridas para su ejecución. Los procedimientos también deben incluir los pasos que se requieren cuando ocurren resultados inesperados.

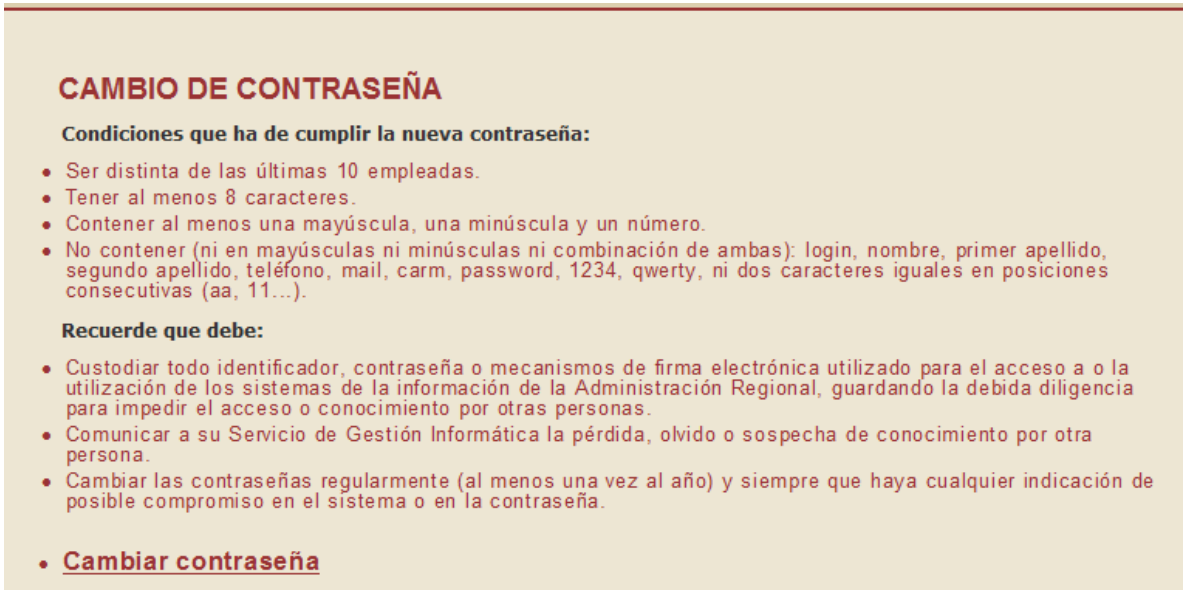
Por ejemplo los procedimientos para contraseñas incluyen los pasos detallados que se requieren para configurar las cuentas y los pasos para cambiar o reiniciar las contraseñas. A continuación se muestra un ejemplo de un procedimiento, en este caso, el procedimiento de alta de un nuevo usuario que a su vez incluye el procedimiento de asignación de contraseñas.



El procedimiento especifica que la primera vez que el usuario vaya a acceder a los sistemas, deberá realizar lo siguiente:

1. Llamar al CAU (368900)

2. El CAU verificará la identidad del usuario.
3. El usuario indicará una contraseña (1) al CAU.
4. El CAU cambia la contraseña del usuario por la contraseña (1) indicada.
5. El usuario accede al sistema con la contraseña (1) y la modifica por otra totalmente diferente. Los requisitos de la contraseña (2) se especifican durante el proceso de modificación.



6. CAU verifica que se ha modificado la contraseña.

Del mismo modo que existe un procedimiento de alta de usuario también existe el procedimiento de baja de un usuario, este procedimiento debe realizarse exhaustivamente y es necesario realizar revisiones periódicas del mismo. El peligro que puede conllevar no seguir los pasos estipulados en este procedimiento está en la posibilidad del acceso a los sistemas de la CARM de un empleado dado de baja con la consecuente fuga de información.

Ejemplo de una mala gestión de un procedimiento de baja

Un usuario X ha notado que desde hace unos días no tiene acceso a su buzón de correo.

Tras realizar las comprobaciones técnicas, el CAU le notifica que ese buzón de correo se encontraba bloqueado tras una revisión de los usuarios dados de baja.

Tras investigar el caso se comprueba que el usuario X llevaba accediendo desde hace 10 años al buzón de correo de otro usuario Y que se llamaba igual que él.

Se comprobó posteriormente que el usuario Y tenía 80 años y que no estaba en activo.

¿Cuáles son los procedimientos de seguridad que han sido mal ejecutados?

Antes de comentar los procedimientos de seguridad mal ejecutados, conviene plantearse la siguiente pregunta;

¿Cómo tenía acceso ese usuario X al uso de la cuenta de correo del usuario Y?

Probablemente el usuario X cuando fue dado de alta en los sistemas de la CARM siguiendo el procedimiento de alta de usuario, se puso en contacto con el CAU para acceder a su cuenta. El fallo estuvo en la verificación que el CAU hizo de este usuario. Al llamarse igual que el otro usuario y no comprobar DNI ni otro tipo de verificación le asigno erróneamente la cuenta de correo de otro usuario que se llamaba igual (usuario Y).

¿Cómo no se enteró el usuario Y que su cuenta de correo no estaba siendo usada por otro usuario?

En realidad este usuario ya no estaba trabajando para la CARM. Este usuario debería haber sido eliminado cuando se dio de baja. El procedimiento de seguridad que se incumplió aquí fue el de baja de usuario.

Los dos procedimientos que presentaban deficiencias y que podrían haber ocasionado problemas con la integridad de la información de la CARM fueron el procedimiento de alta del usuario X y el procedimiento de baja del usuario Y.

¿Cómo se ha detectó este problema?

Este problema fue detectado gracias a la ejecución de otro procedimiento de seguridad, en este caso el *"procedimiento de revisión de derechos de acceso"*.

Los procedimientos de seguridad son los encargados de que el funcionamiento operacional de los procesos asociados a los servicios de la CARM se ejecuten correctamente y no se olvide ningún paso que pueda comprometer la información de la CARM.

6. Protocolos de seguridad.

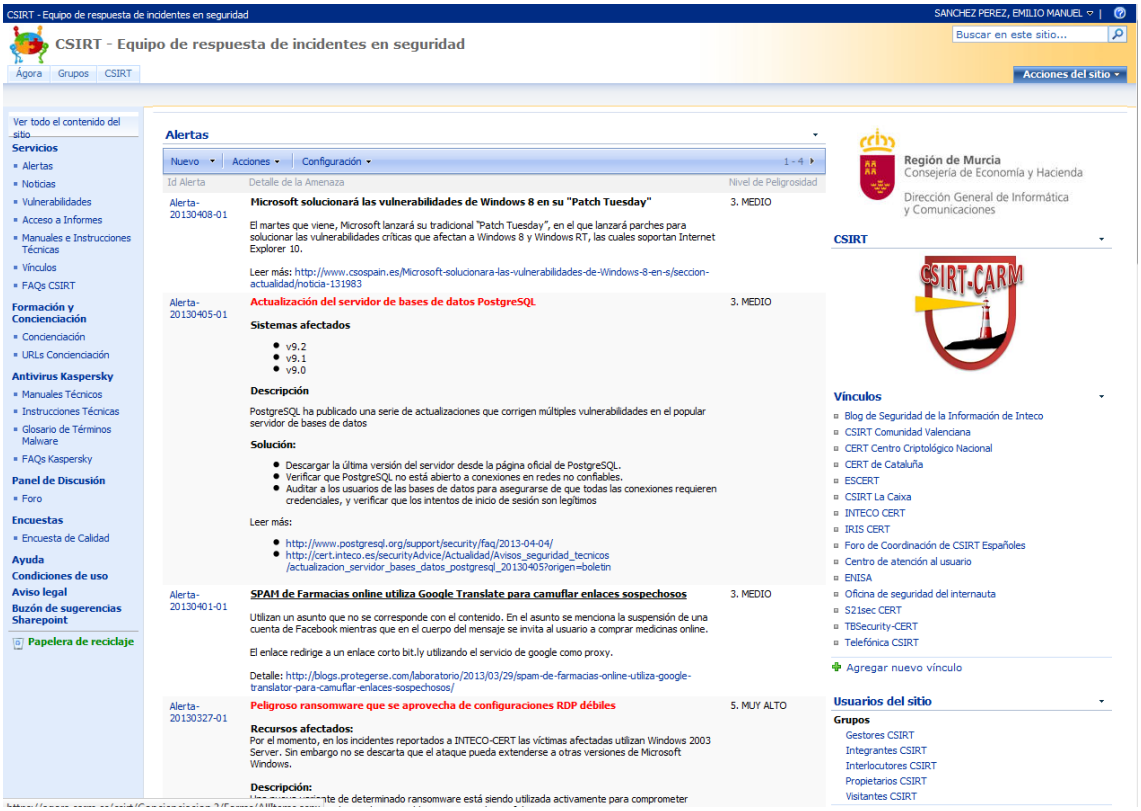
Los protocolos de seguridad deben contener información que ayude a ejecutar los procedimientos. Pueden incluir dependencias, sugerencias y ejemplos, notas aclaratorias de los procedimientos, antecedentes que puede ser de utilidad, herramientas que pueden utilizarse, etc.

Un ejemplo de un protocolo de seguridad son los chequeos que diariamente hacen los departamentos de sistemas, comunicaciones, seguridad, calidad… sobre los servicios de la CARM. Este documento debe contener toda la información necesaria para comprobar que los servicios implicados están operativos y que no han sufrido incidente alguno.

Un ejemplo es el protocolo de seguridad del CSIRT[3] que los integrantes del mismo ejecutan diariamente con el objeto de mantener al tanto a los interlocutores de seguridad de cada organismo de la CARM, informándoles de las vulnerabilidades[4], alertas y/o noticias relacionadas con la seguridad de la información involucrada en los servicios ofrecidos por la CARM. Los miembros del grupo están suscritos a blogs de seguridad del sector, al Instituto Nacional de Tecnologías de la Comunicación, al CERT Gubernamental Español, a otros CSIRT del país así como al CSIRT europeo, tras revisar toda la información se selecciona la información relevante y que pudiera afectar a las aplicaciones de las que hace uso la CARM. Tras filtrar todas las noticias, alertas y vulnerabilidades del sector tecnológico se publican en el portal de ágora donde los interlocutores podrán consultarlas y distribuir la información a sus usuarios.

[3] CSIRT: Equipo de respuesta a incidentes de seguridad de la información.

[4] Vulnerabilidad: Las vulnerabilidades son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo. Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario, denominadas vulnerabilidades de seguridad, en un sistema comprometido.



Portal CSIRT. Detalle Alertas

En la siguiente URL, http://rica.carm.es se puede consultar el "Área de seguridad" de rica;

Cabe destacar el manual de buenas prácticas que se puede consultar en esta sección y el cuál debe tener el usuario siempre presente;

Buenas Prácticas

A continuación le ofrecemos una serie de indicaciones y advertencias dirigidas a la prevención de problemas de seguridad:

- Mantenga sus claves en secreto, no las anote en lugares visibles. No utilice contraseñas fáciles de adivinar, como nombres de personas o fechas, y cámbielas regularmente y siempre que sean conocidas por otros. No las utilice desde puestos públicos (como los ciber-bares, bibliotecas, universidades, puestos de trabajo compartidos, etc.), ni emplee las mismas para entornos de trabajo y personales.

- Los Bancos y Cajas de Ahorros nunca solicitan a sus clientes que revelen sus claves personales y confidenciales mediante teléfono, e-mail o fax. En general nunca introduzca sus claves confidenciales en sistema on-line alguno, a menos de que tenga total seguridad y confianza.

- No descargue ni ejecute ficheros de sitios no confiables ni ejecute anexos de correos electrónicos desconocidos o no solicitados, podrían contener un virus. Desconfíe de enlaces a páginas web remitidos por e-mail, pues podrían llevar a un sitio web impostor (phising). No facilite su cuenta de correo alegremente si no quiere convertirse en objetivo de atacantes.

- Utilice sistemas de protección tales con antivirus y cortafuegos. Mantenga éstos actualizados, así como su sistema operativo, navegador y demás programas.

- Disponga de salvapantallas activado con contraseña, cierre la sesión cuando abandone su equipo y apague éste al concluir la jornada.

- Realice copias de seguridad con cierta frecuencia para evitar la pérdida de datos importantes.

- Asegúrese de comprender y respetar las políticas de seguridad establecidas por la CARM

Y sobre todo, ante cualquier duda, póngase en contacto con su Servicio de Gestión Informática.

7. Marco Legal

Decreto Legislativo 1/2001

Decreto legislativo 1/2001, de 26 de enero, por el que se aprueba el Texto Refundido de la Ley de la Función Pública de la Región de Murcia.

Protección de datos personales y su procesamiento

- Directiva 1995/46/CE, de 24 de octubre, del Parlamento y del Consejo, sobre Protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones
- Directiva 2002/58/CE del parlamento europeo y del consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)
- Directiva 2006/24/CE del Parlamento Europeo y del Consejo del 15 de marzo de 2006 sobre conservación de datos de tráfico en las comunicaciones electrónicas.
- Reglamento (CE) 45/2001 del parlamento europeo y del consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos
- L.O.P.D. 15/1999. Ley orgánica de protección de datos de carácter personal.
    - Real Decreto 1720/2007. Real decreto por el que se aprueba el reglamento de desarrollo de la ley orgánica 15/1999.

Artículo 80 Niveles de seguridad

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81 Aplicación de los niveles de seguridad

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

Letra b) del número 5 del artículo 81 redactada por la disposición adicional cuarta del R.D. 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica («B.O.E.» 29 enero).Vigencia: 30 enero 2010

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Otras leyes de interés:

- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Ley 32/2003, de 3 noviembre, General de Telecomunicaciones
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Incorpora al ordenamiento jurídico español la Directiva 2000/31/CE (8/junio) relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

Incorpora parcialmente la Directiva 98/27/CE (19/mayo) relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de conformidad con lo establecido en ella, una acción de cesación contra las conductas que contravengan lo dispuesto en esta Ley.

Los aspectos con implicación más directa de la LSSICE para cualquier empresa que preste servicios por Internet son:

- La necesidad de comunicar al Registro Mercantil su nombre de dominio.
- La obligación de informar de determinadas características de la empresa en su página Web (denominación social, NIF, domicilio y dirección de correo electrónico, teléfono o fax. Datos de inscripción registral, etc.)
- La regulación de las comunicaciones comerciales electrónicas.

La LSSICE, en su artículo 9, establece la obligación de comunicar al Registro Mercantil el nombre de dominio o dirección de Internet que se emplee para dar información y/o servicios. La Ley, en su Disposición transitoria única (Anotación en los correspondientes registros públicos de los nombres de dominio otorgados antes de la entrada en vigor de esta Ley), da un plazo de un año para efectuar la comunicación (hasta el 12/10/2003).

Artículo 9. Constancia registral del nombre de dominio.

Los prestadores de servicios de la sociedad de la información establecidos en España deberán comunicar al Registro Mercantil en el que se encuentren inscritos, o a aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad, al menos, un nombre de dominio o dirección de Internet que, en su caso, utilicen

para su identificación en Internet, así como todo acto de sustitución o cancelación de los mismos, salvo que dicha información conste ya en el correspondiente registro.

Los nombres de dominio y su sustitución o cancelación se harán constar en cada registro, de conformidad con sus normas reguladoras.

Las anotaciones practicadas en los Registros Mercantiles se comunicarán inmediatamente al Registro Mercantil Central para su inclusión entre los datos que son objeto de publicidad informativa por dicho Registro.

La obligación de comunicación a que se refiere el apartado 1 deberá cumplirse en el plazo de un mes desde la obtención, sustitución o cancelación del correspondiente nombre de dominio o dirección de Internet.

Las empresas que presten servicios de la Sociedad de la Información deben suministrar una determinada información a sus clientes, tal y como establece el artículo 10.

***Artículo 10. Información general**.*

1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.

Los datos de su inscripción en el Registro a que se refiere el artículo 9.

En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

Si ejerce una profesión regulada deberá indicar:

1.- Los datos del Colegio profesional al que, en su caso, pertenezca y nº de colegiado.

2.- El título académico oficial o profesional con el que cuente.

3.- El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

4.- Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

El número de identificación fiscal que le corresponda.

Información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.

Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.

La LSSICE regula también, en los artículos 21 y 22, las comunicaciones comerciales por vía electrónica, prohibiendo las que no hayan sido solicitadas o autorizadas por el destinatario. Asimismo, cuando se recoja la dirección de correo electrónico de una persona, en el caso de que se pretenda utilizarla para efectuar comunicaciones comerciales, se le debe informar y pedir consentimiento para tal cosa.

Artículo 21. Prohibición de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.

Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

Artículo 22. Derechos de los destinatarios de comunicaciones comerciales.

1. Si el destinatario de servicios debiera facilitar su dirección de correo electrónico durante el proceso de contratación o de suscripción a algún servicio y el prestador pretendiera utilizarla posteriormente para el envío de comunicaciones comerciales, deberá poner en conocimiento de su cliente esa intención y solicitar su consentimiento para la recepción de dichas comunicaciones, antes de finalizar el procedimiento de contratación.

2. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente. A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado.Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos

Para consultar de forma íntegra: http://noticias.juridicas.com/base_datos/Admin/l34-2002.html

- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (LISI)

La ley se enmarca en el conjunto de medidas que constituyen el Plan Avanza para el desarrollo de la Sociedad de la Información. Esta ley está dirigida al sector privado.

El Plan Avanza prevé entre sus medidas la adopción de una serie de iniciativas normativas dirigidas a eliminar las barreras existentes a la expansión y uso de las tecnologías de la información y de las comunicaciones y para garantizar los derechos de los ciudadanos en la nueva sociedad de la información.

Esta Ley, por una parte, introduce una serie de innovaciones normativas en materia de facturación electrónica y de refuerzo de los derechos de los usuarios y, por otra parte, acomete las modificaciones necesarias en el ordenamiento jurídico para promover el impulso de la sociedad de la información.

Capítulo I

Introduce sendos preceptos dirigidos a impulsar el empleo de la factura electrónica y del uso de medios electrónicos en los procesos de contratación, así como garantizar una interlocución electrónica de los usuarios y consumidores con las empresas que presten determinados servicios de especial relevancia económica:

- Contratación electrónica bienes/servicios
- Consulta datos de cliente y de facturación
- Presentación de quejas y reclamaciones
- Ejercicio de los derechos ARCO

Capítulo II

Engloba las modificaciones legislativas que se han estimado necesarias para promover el impulso de la sociedad de la información y las comunicaciones electrónicas, en particular:

- Ley 34/2002 de Servicios de la Sociedad de la Información y del Comercio Electrónico
- Ley 59/2003 de Firma Electrónica
- Ley 32/2003 General de Telecomunicaciones

El artículo 2 de la ley de Impulso de la Sociedad de la Información, se refiere a la obligación de disponer de un medio de interlocución telemática para la prestación de servicios al público de especial trascendencia económica. A continuación se amplía el contenido del artículo 2.

1. Sin perjuicio de la utilización de otros medios de comunicación a distancia con los clientes, las empresas que presten servicios al público en general de especial trascendencia económica deberán facilitar a sus usuarios un medio de interlocución telemática que, mediante el uso de certificados reconocidos de firma electrónica, les permita la realización de, al menos, los siguientes trámites:

a) Contratación electrónica de servicios, suministros y bienes, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico entre las partes, sin perjuicio de lo establecido en la normativa sectorial.

b) Consulta de sus datos de cliente, que incluirán información sobre su historial de facturación de, al menos, los últimos tres años y el contrato suscrito, incluidas las condiciones generales si las hubiere.

c) Presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, garantizando la constancia de su presentación para el consumidor y asegurando una atención personal directa.

d) Ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal.

2. A los efectos de lo dispuesto en el apartado anterior, tendrán la consideración de empresas que presten servicios al público en general de especial trascendencia económica, las que agrupen a más de cien trabajadores o su volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, exceda de 6.010.121,04 euros y que, en ambos casos, operen en los siguientes sectores económicos:

a) Servicios de comunicaciones electrónicas a consumidores, en los términos definidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

b) Servicios financieros destinados a consumidores, que incluirán los servicios bancarios, de crédito o de pago, los servicios de inversión, las operaciones de seguros privados, los planes de pensiones y la actividad de mediación de seguros. En particular, se entenderá por:

1. Servicios bancarios, de crédito o de pago.

2. Servicios de inversión. 3. Operaciones de seguros privados.

4. Planes de pensiones.

5. Actividad de corredor de seguros.

c) Servicios de suministro de agua a consumidores, definidos de acuerdo con la normativa específica.

d) Servicios de suministro de gas al por menor.

e) Servicios de suministro eléctrico a consumidores finales.

f) Servicios de agencia de viajes.

g) Servicios de transporte de viajeros por carretera, ferrocarril, por vía marítima, o por vía aérea, de acuerdo con lo dispuesto en la normativa específica aplicable.

h) Actividades de comercio al por menor.

3. Excepcionalmente, el Gobierno o, en su caso, los órganos competentes de las Comunidades Autónomas podrán ampliar el ámbito de aplicación del apartado 1 del presente artículo a otras empresas diferentes de las previstas en la Ley, en aquellos casos en los que, por la naturaleza del servicio que presten, se considere que en el desarrollo de su actividad normal deban tener una interlocución telemática con sus clientes o usuarios.

En el plazo de un año desde la entrada en vigor de la obligación a que se refiere el apartado 1, el Gobierno analizará la aplicación del apartado 2 de este artículo a otras empresas con más de cien trabajadores o que tengan un volumen anual de operaciones, calculado conforme a lo establecido en la normativa del Impuesto sobre el Valor Añadido, superior a 6.010.212,04 euros, que en el desarrollo de su actividad normal, presten servicios en los que se considere que deban tener una interlocución telemática con sus clientes o usuarios.

Las Comunidades Autónomas con competencias exclusivas en las materias objeto de obligación de comunicación telemática podrán modificar el ámbito y la intensidad de aplicación del apartado 1 del presente artículo en aquellos casos en que precisamente debido al desarrollo sectorial de sus competencias lo consideren oportuno.

Para consultar la ley íntegra: http://www.boe.es/buscar/doc.php?id=BOE-A-2007-22440

- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP)

La Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos mencionada a veces por sus siglas LAECSP es una ley española que reconoce a los ciudadanos su derecho a relacionarse electrónicamente con las administraciones públicas, así como la obligación de éstas a garantizar ese derecho.

De forma general, es una ley que pretende reglamentar todos aquellos aspectos relacionados con el procedimiento administrativo para permitir que éste sea llevado a cabo en un contexto electrónico. Las implicaciones de dicha Ley afectan de modo general a la práctica totalidad de las actividades de las Administraciones Públicas.

Exposición de motivos. (…) Es en ese contexto en el que las Administraciones deben comprometerse con su época y ofrecer a sus ciudadanos las ventajas y posibilidades que la sociedad de la información tiene, asumiendo su responsabilidad de contribuir a hacer realidad la sociedad de la información. Los técnicos y los científicos han puesto en pie los instrumentos de esta sociedad, pero su generalización depende, en buena medida, del impulso que reciba de las Administraciones Públicas. Depende de la confianza y seguridad que genere en los ciudadanos y depende también de los servicios que ofrezca.

El mejor servicio al ciudadano constituye la razón de la reformas que tras la aprobación de la Constitución se han ido realizando en España para configurar una Administración moderna que haga del principio de eficacia y eficiencia su eje vertebrador siempre con la mira puesta en los ciudadanos. Ese servicio constituye también la principal razón de ser de la Ley de acceso electrónico de los ciudadanos a los servicios públicos que trata, además, de estar a la altura de la época actual. (…)

(…) una Ley para el acceso electrónico de los ciudadanos a las Administraciones Públicas se justifica en la creación de un marco jurídico que facilite la extensión y utilización de estas tecnologías. Y el principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones (TIC) en la sociedad en general y en la Administración en particular es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización. La desconfianza nace de la percepción, muchas veces injustificada, de una mayor fragilidad de la información en soporte electrónico, de posibles riesgos de pérdida de privacidad y de la escasa transparencia de estas tecnologías. (…)

Objeto de la Ley.

1. La presente Ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos y regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas con la finalidad de garantizar sus derechos, un tratamiento común ante ellas y la validez y eficacia de la actividad administrativa en condiciones de seguridad jurídica.

2. Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

Para consultar la ley íntegra: http://www.boe.es/buscar/doc.php?id=BOE-A-2007-12352

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional Seguridad.

Artículo 10. La seguridad como función diferenciada.

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

Artículo 197

1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en este artículo, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

6. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

7. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

8. Si los hechos descritos en los apartados anteriores se cometiesen en el seno de una organización o grupo criminales, se aplicarán respectivamente las penas superiores en grado.

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad.

Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007 (sólo para la AGE y sus organismos)

8. ANEXO A: Glosario

Los términos que se emplean en esta orden tendrán el significado que se establece en el anexo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en el anexo IV del Real decreto 3/2010, de 8 de enero , por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica y en el anexo del Real decreto 4/2010, de 8 de enero , por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.

En el ámbito específico de la administración regional se establecen las siguientes definiciones:

a) Usuario: cualquier persona dentro de los sistemas de información de personal de la Administración Regional.

b) Dirección IP corporativa: cualquier etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo o medio electrónico que utiliza el protocolo IP dentro de la red de telecomunicaciones corporativa.

c) Uso aceptable: pautas de comportamiento de los usuarios de la red corporativa considerada adecuada y pertinente en relación al desempeño de su trabajo.

d) Uso no aceptable: pautas de comportamiento de los usuarios de la red corporativa considerada o bien no adecuada en relación al desempeño de su trabajo o bien constitutiva de presuntas acciones delictivas tipificadas por el Código Penal.

e) Contenidos inapropiados e ilícitos: Aquellos contenidos que infringen la legislación vigente o no se consideran permitidos dentro de la Red de comunicaciones corporativa.

f) Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante la familia de protocolos de comunicaciones TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

9. Bibliografía.

https://www.ccn-cert.cni.es/

http://www.inteco.es/

http://www.inteco.es/blogs/inteco/Seguridad/BlogSeguridad/ultimos_articulos/

https://www.csirt.es/

http://www.rediris.es/cert/

http://escert.upc.edu/

http://www.csirtcv.gva.es/

https://www.cesicat.cat/

http://csirt.org/

http://noticias.juridicas.com/