ÍNDICE

1. OBJETIVO

La presente normativa ha sido aprobada por el Consejo de Administración de esta empresa en fecha 13 de junio de 2024 y entrará en vigor al día siguiente de su aprobación, hasta que sea remplazada por una modificación o una nueva normativa.

2. REVISIÓN Y/O ACTUALIZACIÓN

Con periodicidad anual se revisará el contenido y en caso de que sea necesario se procederá a su modificación, que deberá de ser aprobada por los órganos anteriormente indicados, y tendrán que ser difundidas entre las personas afectadas por estas.

3. OBJETO

El objeto del presente documento es establecer la normativa de uso seguro de los medios electrónicos en SMAP, dentro del alcance señalado en el Esquema Nacional de Seguridad.

Los sistemas de información son elementos básicos para el desarrollo de la actividad de SMAP. Estos medios se ponen a disposición de las personas usuarias como instrumentos de trabajo para el ejercicio de su actividad profesional. Motivo por el cual cabe utilizar estos recursos de manera responsable mediante el seguimiento de normas y buenas prácticas que salvaguarden la seguridad de la información, los sistemas informáticos y los recursos tecnológicos proporcionados por la entidad.

4. ALCANCE

Mediante esta normativa, la SMAP establece la regulación del uso de los medios electrónicos del sistema de información (incluido el acceso remoto a estos), a través del establecimiento de medidas de cumplimiento obligatorio para todo el personal, y quedan sujetos a esta, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición.

El personal de terceros (empresas proveedoras, convenios, etc.) con acceso al sistema quedan también sujetos a esta, en la medida que le sean aplicables, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición de estas personas usuarias para el ejercicio de sus actividades en la SMAP.

De ahora en adelante, se utilizará “el Usuario” para referirse al personal propio o de terceros.

5. CANAL DE SOLICITUDES Y/O NOTIFICACIONES

Las solicitudes de autorización y las notificaciones reflejadas en esta normativa se dirigirán al departamento de informática (informatica@smap.palma.cat) quien será el responsable de aceptarlas, previa aprobación –si corresponde- por el responsable del departamento.

6. INCIDENTES DE SEGURIDAD

Cuando un Usuario detecte cualquier anomalía (mal funcionamiento, aplicaciones que no arranquen o que se cierren de manera inesperada, pérdida de documentos, de memorias USB, etc.) o incidente de seguridad (virus, suplantación de identidad, pérdidas de clave, etc.) que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de SMAP o pueda dañar su imagen, tiene que informar inmediatamente (informatica@smap.palma.cat).

7. NORMATIVA DE USO DE LOS MEDIOS ELECTRÓNICOS

7.1. NORMAS DE UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE COMUNICACIONES

Cualquier persona que precise un nuevo soporte tendrá que remitir la solicitud al departamento informático mediante correo electrónico a (informatica@smap.palma.cat) indicando el motivo o necesidad. El responsable aceptará, denegará o remitirá al correspondiente responsable para su aceptación.

Estas normas conciernen específicamente a todos los dispositivos facilitados y configurados por SMAP, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidad de acceso a los sistemas de información.

La SMAP proporcionará al personal, el equipamiento debidamente configurado con acceso a los servicios y las aplicaciones que sean necesarias para el ejercicio de sus funciones.

En cuanto a los cuales aplicará las normas generales y para los equipos portátiles y dispositivos móviles aplicará las normas específicas para este tipo de equipamiento.

7.1.1. NORMAS GENERALES

Los equipos se deben utilizar únicamente para fines institucionales/profesionales y como herramienta para el ejercicio de las tareas encomendadas. Cada equipo estará asignado a una única persona. Esta persona es responsable de su uso correcto. Cuando el trabajador que hace uso del dispositivo abandona su puesto de trabajo, deberá dejar el dispositivo bloqueado y en buenas condiciones.

Salvo autorización expresa, no se dispondrán de privilegios de administrador sobre los equipos.

Únicamente el personal autorizado podrá distribuir, instalar o desinstalar software y maquinaria, o modificar la configuración de cualquiera de los equipos.

Cuando sea necesario instalar equipos que no hayan sido proveídos por SMAP, se debe solicitar autorización previa.

Las personas usuarias tendrán que notificar, lo antes posible, cualquier comportamiento anómalo de sus equipos (va lento, no arranca, no funciona correctamente, etc.),

especialmente cuando haya sospechas de que se haya producido algún incidente de seguridad. De la misma manera tendrá que comunicar la ausencia de cables y/o accesorios o cualquier otra evidencia de deterioro.

Con carácter general, no se permite el uso de dispositivos propios, "BYOD (Bring Your Own Device)", para el acceso o almacenamiento de información excepto autorización expresa.

No se puede hacer uso de los dispositivos en horario no laboral y fuera de las instalaciones o punto de trabajo propio de la persona trabajadora, a excepción del personal que dispone de dispositivos móviles localizables sin limitación horaria.

Con la finalidad de cumplir con la normativa de protección de datos y respecto a los derechos de todos los compañeros, no se permite la grabación de las conversaciones siendo responsabilidad de cada trabajador seguir las pautas indicadas y quien tendrá que responder de las responsabilidades que se puedan derivar.

7.1.2. NORMAS ESPECÍFICAS PARA EQUIPOS PORTÁTILES Y DISPOSITIVOS MÓVILES

Para los portátiles y móviles además de las normas generales, son aplicables las siguientes:

- Estos dispositivos estarán, en todo momento, bajo la custodia de la persona usuaria que los utilice, que será la responsable de adoptar las medidas necesarias para evitar daños o sustracción, así como del acceso por parte de personas no autorizadas.
- La sustracción de estos equipos se tiene que notificar inmediatamente para la adopción de las medidas que correspondan.
- Se debe solicitar autorización cuando se usen para conectarse remotamente a través de redes que no estén bajo el control de SMAP o que no hayan sido autorizadas, autorización que se hará extensible también a los servicios a los cuales se accede.
- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, la persona usuaria lo devolverá, a fin de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a una persona nueva.

7.2. NORMAS PARA EL ALMACENAMIENTO DE INFORMACIÓN Y COPIAS DE SEGURIDAD

Para garantizar la disponibilidad de la información delante de un incidente de seguridad, de forma periódica se hacen copias de seguridad de las carpetas del servidor propio de la SMAP (NAS).

Por este motivo, los Usuarios tendrán que almacenar en estos los datos generados en el ejercicio de sus competencias profesionales. Respecto de esto, se informa que no se hacen copias de seguridad de la información que no se encuentren en las unidades indicadas.

No se permite el almacenamiento de información privada ni de terceros ajenos a los recursos indicados.

La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente de seguridad. Para recuperar esta información habrá que dirigir una solicitud de restauración.

7.3. NORMAS DE USO PARA SOPORTES DE ALMACENAMIENTO EXTRAÍBLES

Como norma general, en la SMAP el uso de soportes o medios de almacenamiento extraíbles (memorias USB, discos duros, etc.) no está autorizado. Para utilizarlos se deberá contar con la debida autorización del departamento de informática.

En el supuesto de que a la persona usuaria se le autorice el uso de este tipo de soportes de trabajo, las normas a observar son las siguientes:

- Como norma general, se harán servir los soportes extraíbles proporcionados por la SMAP. Estando destinados a un uso exclusivamente profesional, como herramienta de transporte puntual de ficheros, no como herramienta de almacenamiento. En estos soportes se deben aplicar medidas de seguridad (contraseña, encriptación...) para evitar accesos de terceros no autorizados.
- El uso de medios de almacenamiento extraíbles particulares no está autorizado, salvo que se disponga de la autorización debida.
- Su uso no está autorizado para el almacenamiento de datos personales, salvo que se disponga de la autorización debida.

Este tipo de dispositivos se tendrán que almacenar en lugares seguros, para prevenir robos o el acceso de terceros no autorizados. La pérdida o la sustracción de estos dispositivos, con indicación del contenido, se tiene que poner en conocimiento, de manera inmediata.

El transporte de estos soportes fuera de las instalaciones de SMAP la tiene que hacer exclusivamente personal autorizado, autorización que contempla igualmente la información que sale. En este caso, se deberá enviar una solicitud para que se os asesore sobre las medidas de seguridad que se deberán implementar.

7.3.1. NORMAS PARA EL BORRADO Y LA ELIMINACIÓN DE SOPORTES INFORMÁTICOS

Los medios de almacenamiento que, por obsolescencia o degradación, pierdan la utilidad, y especialmente aquellos que contengan datos de carácter personal, se tienen que eliminar de manera segura para evitar accesos a esta información. En este sentido, la persona usuaria deberá de tener en cuenta las siguientes indicaciones:

- Aseguraros que el contenido del soporte puede ser eliminado.
- Cualquier petición de eliminación de soporte informático se deberá solicitar.

Para la reutilización de medios de almacenamiento, para otros fines diferentes de los que originaron el uso, se debe solicitar un borrado seguro.

7.4. NORMAS RESPECTO A LA GESTIÓN DE DOCUMENTOS

7.4.1. IMPRESORAS EN RED, FOTOCOPIADORAS/ESCÁNERS

Con carácter general, se tienen que utilizar las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, se pueden instalar impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente.

En ningún caso se podrá hacer uso de impresoras, fotocopiadoras que SMAP no haya proporcionado. En relación a los sistemas de copia e impresión y documentación impresa, los Usuarios tienen que seguir las directrices siguientes:

- Los documentos, con carácter general, se generarán en formato electrónico, pudiendo digitalizar aquellos que no sean susceptibles de ser generados en este formato.
- Cuando se imprimen documentos, en sistemas de impresión o copias comunes, estos tienen que permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a ellos.
- En la realización de copias de seguridad y/o escaneo, no olvidar retirar los originales.
- En caso de encontrarse documentación en un sistema de copia o impresión, el Usuario intentará localizar a la persona propietaria para que proceda a la recogida inmediata. En caso de desconocer a la persona propietaria o no estar localizable, lo pondrá inmediatamente en conocimiento.
- Para evitar un uso excesivo de los recursos, mejorando el impacto medioambiental en la generación de documentos en papel, y por motivos de seguridad, antes de imprimir documentos, el Usuario se tiene que asegurar que sea necesario hacerlo.

7.4.2. CUIDADO Y PROTECCIÓN DE LA DOCUMENTACIÓN IMPRESA

La documentación tiene que ser protegida, de manera que solo tenga acceso el personal autorizado, a tal efecto la persona usuaria tendrá en cuenta las siguientes medidas:

- Los lugares de trabajo permanecerán claros, sin más material sobre la mesa que el requerido para la actividad que se está realizando en cada momento.

- Cuando no sea utilizada se deberá guardar en sistemas de almacenamiento (armarios o archivadores) preferentemente con llave. No podrán ser publicados en tablones o similares.
- Cuando los documentos no sean necesarios, tienen que ser eliminados utilizando los medios puestos a disposición por parte de la entidad (destructora de documentos), de manera que no sea recuperable la información que puedan contener.
- Antes de abandonar las salas de reuniones o permitir que alguien ajeno acceda, se limpiarán adecuadamente las pizarras y se recogerán todos los documentos, teniendo cuidado que no quede ningún tipo de información "sensible" o "interna" accesible a personas no autorizadas.

7.5. PUESTO DE TRABAJO NEGRO

Los puestos de trabajo tienen que permanecer claros, sin más material sobre la mesa que el requerido para la actividad que se está haciendo en cada momento.

7.6. ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS TRATADOS

Para acceder a los sistemas y recursos informáticos se debe tener asignada previamente una cuenta de usuario. El alta de los usuarios será solicitada y autorizada según las políticas de SMAP. La autorización del acceso establecerá el perfil necesario con el que se configuren las funcionalidades y los privilegios disponibles en las aplicaciones según las competencias de cada persona, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

Los usuarios dispondrán de credenciales personales de acceso (código de usuario y una contraseña, certificado electrónico, etc.) para el acceso a los sistemas de información de SMAP utilizando la red segura, protegida con los servicios de seguridad destinados a tal efecto. Responsables de su custodia y de toda la actividad relacionada con el uso de su acceso autorizado, respecto de los cuales se deberá observar las siguientes medidas:

- El código de usuario es único para cada persona, intransferible e independiente del PC o terminal desde el que se realiza el acceso.
- Los usuarios no tienen que revelar o entregar, bajo ningún concepto, las credenciales de acceso a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros. De la misma manera, no tienen que utilizar ningún acceso autorizado de otra persona, aunque dispongan de la autorización de su titular.
- Si una persona tiene sospechas de que sus credenciales están siendo utilizados por otra persona, lo tiene que comunicar inmediatamente.
- Las personas usuarias tienen que utilizar contraseñas seguras, de acuerdo con la política establecida en SMAP, no tiene que estar compuestas únicamente por palabras del diccionario o de otros fácilmente predecibles o asociables a la persona usuaria (nombres de la familia, direcciones, matrículas de coche, teléfonos,

nombres de productos comerciales u organizaciones, identificadores de usuarios, de grupo o del sistema, DNI, etc.).

- Los sistemas que así lo permitan, forzarán el cambio de contraseña al menos una vez al año, previo aviso con los días de antelación suficientes. En los que no sea posible, será responsabilidad de los usuarios proceder al cambio con esta periodicidad.

7.7. ACCESO A UNA CUENTA DE UN USUARIO EN SU AUSENCIA O BAJA

Cuando sea necesario acceder a la carpeta personal o cuenta de correo corporativo de un Usuario, este acceso se deberá hacer contando con la autorización del responsable o por la persona en que esta delegue.

En caso de que no resulte posible solicitar esta autorización (muerte, enfermedad, imposibilidad de localización, etc.), el acceso podrá ser realizado siempre que esté autorizado de forma expresa por el responsable del mismo o por la persona en que esta delegue.

En ambos casos, se tendrá que motivar la necesidad de acceso y ser comunicada al responsable del Usuario, que elaborará un acta en la que se recojan todas las acciones llevadas a cabo.

7.8. CONFIDENCIALIDAD, PROTECCIÓN DE DATOS PERSONALES Y DEBER DE SECRETO

La información contenida en el Sistema de Información de SMAP es responsabilidad de esta entidad, por lo cual las personas usuarias tiene que abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) esta información, excepto autorización expresa de la propia institución. Además, tendrá que tener en cuenta las siguientes premisas:

- Todos los Usuarios, que por razón de su actividad profesional hayan tenido acceso a información gestionada por SMAP (documentos, metodologías, claves, análisis, programas, etc.) tendrán que mantener, por tiempo indefinido, una reserva absoluta.
- Los usuarios solo podrán acceder con las debidas autorizaciones a aquella información necesaria para el ejercicio de sus tareas. En todo caso, no se tiene que acceder a información sin las autorizaciones debidas.
- Toda la información contenida en los sistemas de información de SMAP o que circule por las redes de comunicación se tiene que utilizar únicamente para el cumplimiento de las funciones que tiene encomendadas el Usuario.
- Los derechos de acceso de los usuarios a la información y a los sistemas de información que la traten, siempre se deberán otorgar en base a los principios de

"mínimo privilegio", "necesidad de conocer y responsabilidad de compartir" y "capacidad de autorizar".

- La información que comprenda datos de carácter personal quedará afectada también por la normativa vigente en materia de Protección de Datos Personales, estando obligado a guardar secreto sobre estas, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con SMAP.

7.9. LIMPIEZA DE METADATOS Y DATOS OCULTOS DE LOS DOCUMENTOS ELECTRÓNICOS

Se define metadato como información estructurada que describe, explica, localiza y, además, hace más fácil recuperar, utilizar o gestionar un recurso de información. Los metadatos son comúnmente llamados "datos sobre los datos" o "información sobre la información".

Se define información o datos ocultos como aquellos datos existentes en el contenido de los documentos electrónicos, que no son visibles con la configuración estándar o configuración por defecto de los programas utilizados para su creación y tratamiento, y hay que aplicar alguna opción específica dentro de la configuración de estos programas, para visualizarlos. Un ejemplo de datos ocultos es el texto oculto, filas o columnas ocultas, comentarios o información del documento, etc.

Cuando hacemos una fotografía o creamos documentos con aplicaciones de Microsoft Office (Word, Excel, PowerPoint, etc.) y/o fotografías, estos archivos llevan integrados en sus propiedades una serie de datos ocultos y/o metadatos, como pueden ser el nombre de la persona que ha creado el documento, el programa con el que se ha generado, la fecha de creación, la de modificación, etc. Esto puede perjudicar la confidencialidad de la información y la buena imagen de la entidad.

Todos los archivos electrónicos (documentos ofimáticos, hojas de cálculo, imágenes, etc...) pueden tener integrados en sus propiedades una serie de datos ocultos y/o metadatos, como pueden ser el nombre de la persona que ha creado el documento, el programa con el que se ha generado, la fecha de creación, la de modificación, etc.

Los metadatos contenidos en los ficheros pueden llegar a afectar tanto a la seguridad de la información como a la imagen de SMAP. Por eso, todo archivo que tenga que ser difundido internamente, remitido electrónicamente a un tercero o publicado en Internet (página web, sede electrónica, etc...), tendrá que ser revisado para determinar los metadatos asociados a este, procediendo a su modificación o supresión, para asegurar que no consten datos personales o confidenciales.

7.10. USO DEL CORREO ELECTRÓNICO CORPORATIVO

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios del sistema de información de SMAP para el envío y la recepción de correos electrónicos mediante el uso de cuentas de correo corporativas. Como se trata de un recurso compartido, un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todas las personas.

El correo electrónico se tendrá que utilizar en base al sentido común y teniendo en cuenta la responsabilidad y funciones ejercidas, tratando en cualquier caso de no poner en compromiso ni los sistemas ni la imagen de SMAP.

SMAP queda facultada para filtrar el contenido del correo electrónico de la cuenta de correo proporcionada para el desarrollo de sus funciones laborales, a fin de prevenir virus o en caso de que haya razones fundamentadas en una firme sospecha para SMAP sobre la existencia de actividades delictivas o dolosas del personal.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de esta normativa.

Se podrá insertar contenido adicional a los mensajes enviados a fin de advertir a los receptores de los requisitos legales y de seguridad que tendrán que cumplir en relación con estos correos.

Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o aprovechar las vulnerabilidades. Por este motivo, se establecen las directrices siguientes con el objetivo de reducir el riesgo en el uso del correo electrónico:

- Utilizar el correo electrónico exclusivamente para propósitos profesionales.
- No se tiene que ceder el uso de la cuenta de correo a terceras personas.
- Informar de correos con virus, phishing, malware (programa maligno), etc., sin reenviarlos, para evitar su posible propagación.
- No responder a mensajes de Spam.
- Asegurar la identidad del remitente antes de abrir un mensaje.
- No ejecutar ficheros adjuntos sospechosos. No se tienen que ejecutar los ficheros adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso.

En cuanto al uso del correo electrónico, queda terminantemente prohibido:

- Falsificar, esconder, suprimir o sustituir la identidad del emisor en cualquier correo electrónico.
- Leer o acceder a correos electrónicos ajenos, sin autorización previa.
- Enviar correos electrónicos que contengan en el cuerpo o en los adjuntos información con datos de categorías especiales de datos o datos especialmente sensibles (es decir, salud, ideología, religión, creencias, origen racial, étnico, etc.) o aquellos considerados como de especial protección para SMAP, salvo que se cuente con la autorización pertinente y se hayan aplicado las medidas de seguridad oportunas (cifrado o similares).

7.11. ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN

El acceso corporativo a Internet es un recurso centralizado que SMAP pone a disposición de los Usuarios, como herramienta necesaria para acceder a contenidos y recursos de Internet y como soporte al ejercicio de su actividad profesional. SMAP velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y la productividad del personal, como desde los riesgos de seguridad asociados a su uso. Las normas de uso son las siguientes:

- Como norma general, las conexiones que se hagan a Internet tienen que obedecer a fines profesionales.
- Solo se podrá acceder a Internet mediante los navegadores suministrados y configurados en los puestos de usuario. No se podrá alterar la configuración, ni utilizar un navegador alternativo, sin contar con la debida autorización.
- El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código nocivo.
- Se tendrá que notificar cualquier anomalía (redirección a páginas solicitadas, aviso de lugar no seguro, en páginas habitualmente utilizadas, etc.) detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con este acceso.

Se consideran usos prohibidos, que implican un riesgo de seguridad, las siguientes actuaciones:

- La descarga de programas informáticos sin autorización previa o ficheros con contenido nocivo que supongan una fuente de riesgos para SMAP. En todo caso, aseguraros que el sitio web visitado es fiable.
- El acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas con contenidos ilegales, nocivos, inadecuados o que atenten contra la moral y las buenas costumbres y, en general, de todo tipo de contenidos que incumplen las normas éticas y de cortesía de SMAP.
- El acceso a recursos y páginas web, o la descarga de programas o contenidos que vulneren la legislación en materia de propiedad intelectual.
- La utilización de aplicaciones o herramientas (especialmente el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no estén expresamente autorizados.

7.12. CONEXIÓN REMOTA

Solo se pueden hacer conexiones remotas, siempre y cuando se disponga de la correspondiente autorización del responsable del departamento, previa ponderación de la necesidad de estos accesos.

Los accesos remotos se deberán realizar garantizando que la conexión es segura y cumple con los parámetros establecidos en esta norma. No se podrá realizar utilizando conexiones wifi públicas o no seguras.

Será necesario, en el caso de que se permita el teletrabajo, disponer de la correspondiente autorización del IMI mediante los protocolos establecidos, El IMI facilitará una VPN y certificado de seguridad que se tiene que descargar todo usuario que quiera conectarse remotamente a su puesto de trabajo. La responsabilidad de disponer de un equipo con las características mínimas que requiere el IMI, así como del cuidado y la actualización del mismo es del propio usuario. También cabe destacar que es el usuario quien tiene que tener cuidado de la protección del equipo y de la protección de datos que implica.

Si en la prestación de los servicios, implica la conexión a un soporte o equipo de otro compañero, será necesaria su petición previa para solucionar esta incidencia sin que se pueda acceder a aquellos espacios o carpetas que no se precisen para la resolución de la incidencia. Como norma general, está prohibido activar la cámara o micrófono del soporte al que se conecta con la excepción que se trate de revisar este recurso de cámara o micrófono. En cualquier caso, antes de su activación habrá que informar de forma expresa y clara para que sea comprensible para el usuario.

El departamento de informática podrá realizar tareas de mantenimiento y actualización de los sistemas de forma remota, accediendo a los soportes, carpetas y aplicaciones que sean necesarias para la realización de las tareas profesionales asignadas.

7.13. DERECHOS DE PROPIEDAD INTELECTUAL

Los usuarios y administradores tienen que respetar las condiciones de licencia y copyright del software que usen en sus equipos. Todo software adquirido de forma central por la SMAP deberá estar debidamente licenciado.

Se limita el número de usuarios que pueden ostentar la condición de administrador del sistema y por lo tanto, con capacidad para instalar software, quien tendrá que respetar los derechos de propiedad intelectual de cualquier aplicación y/o software a aplicar.

8. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

La SMAP por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que a este efecto establece la legislación vigente:

- Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y las redes de comunicación de su responsabilidad.
- Monitorizará los accesos a la información contenida en sus aplicaciones.
- Auditará la seguridad de las credenciales y aplicaciones.
- Monitorizaréis los servicios de internet, correo electrónico y otras herramientas de colaboración.

Esta supervisión se realizará en todo caso con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral y otras disposiciones que resulten aplicables, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento la persona que actúa.

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplen los requisitos mínimos de seguridad, pueden ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de esta normativa. Se podrá insertar contenido adicional a los mensajes enviados a fin de advertir a los receptores de los requisitos legales y de seguridad que deberán cumplir en relación con estos correos.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código nocivo. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y medida de los ficheros descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar sobre usos prolongados e indebidos del servicio.

9. INCUMPLIMIENTO DE LA NORMATIVA

Los usuarios del sistema de información de SMAP están obligados a cumplir lo que prescribe esta “Normativa de Uso de Medios Electrónicos”.

En caso de que una persona usuaria no observe alguno de los preceptos señalados en esta normativa, sin perjuicio de las acciones disciplinarias y administrativas que sean procedentes y, si procede, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos que tengan asignados, previa instrucción del procedimiento legal que corresponda.

En el caso de personal de terceros, el incumplimiento de esta normativa podría derivar en la imposición de penalidades pudiendo llegar incluso a la resolución del contrato, siguiendo el procedimiento establecido a este efecto en la normativa sobre contratación administrativa.