SCAYLE | Junta de Castilla y León

SGSI-NOR-01

NORMATIVA DE SEGURIDAD

Índice

1. OBJETIVO

La presente Normativa de Seguridad define el conjunto de principios básicos y requisitos de seguridad que son de obligado cumplimiento conforme a lo dispuesto en el Anexo II del **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).**

Los Sistemas de Información constituyen elementos básicos para el desarrollo de las misiones encomendadas a SCAYLE, por lo que los usuarios deben utilizar estos recursos de manera que se preserven en todo momento las cinco dimensiones de seguridad sobre las informaciones manejadas y los servicios prestados: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

La utilización de recursos tecnológicos para el tratamiento de la información tiene una doble finalidad para SCAYLE:

- Facilitar y agilizar el desarrollo de las tareas habituales de SCAYLE.
- Proporcionar información completa, homogénea, actualizada y fiable.

La utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización. Los usuarios disponen de estos medios y recursos como instrumentos de trabajo para su actividad profesional, por eso compete a SCAYLE determinar las normas, condiciones y responsabilidades bajo las que se deben utilizar esos recursos tecnológicos.

Por tanto, la presente Normativa de Seguridad pretende establecer los lineamientos para alcanzar la mayor eficacia y seguridad en su uso. Por otra parte, cabe destacar que este documento contiene información importante para garantizar la seguridad de nuestros sistemas de información, por lo que la difusión de su contenido está limitada al personal que lo necesite para el desarrollo de sus funciones. Este documento se considera de uso público de SCAYLE y, por consiguiente, se podrá redistribuir en la página web, y demás sistemas de información que se consideren adecuados.

2. ÁMBITO DE APLICACIÓN

La presente Normativa de Seguridad se aplica **a todos los sistemas de SCAYLE, centros de trabajo y recursos materiales e informáticos**; sus contenidos traen causa de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la Entidad. Esta Normativa deberá estar permanentemente actualizada y las normas que contiene son de **obligado cumplimiento** para toda persona que preste o use servicios en SCAYLE, incluyendo **personal interno**, **personal de proveedores externos y clientes o usuarios de servicios,** cuando sean usuarios de los Sistemas de Información de SCAYLE.

En el ámbito de la presente Normativa, se entiende por **usuario** cualquier empleado perteneciente o ajeno a SCAYLE, así como personal de organizaciones públicas o privadas externas, entidades colaboradoras o cualquier otro personal con algún tipo de vinculación con SCAYLE y que utilice o tenga acceso a los Sistemas de Información de SCAYLE.

3. VIGENCIA

La presente Normativa de Seguridad de SCAYLE ha sido aprobada por el **Comité de Seguridad**, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos de tratamiento de información que SCAYLE pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación entrará en vigor inmediatamente después de su aprobación por el Comité de Seguridad de SCAYLE.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa de Seguridad.

4. REVISIÓN Y EVALUACIÓN

La gestión de esta Normativa de Seguridad corresponde al **Responsable de Seguridad** de SCAYLE que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Anualmente el Responsable de Seguridad revisará la presente Normativa de Seguridad, que se someterá, de haber modificaciones, a la aprobación del Comité de Seguridad de SCAYLE.

La revisión se orientará, tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información y protección de datos, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc. El Responsable de Seguridad, será la persona encargada de asegurar la custodia en los lugares dedicados a ello y divulgación de la versión aprobada de este documento.

5. CONTEXTO NORMATIVO DE REFERENCIA

REFERENCIA	CONTEXTO	DESCRIPCIÓN
RD 311/2022	Nacional	Por el que se regula el Esquema Nacional de Seguridad (ENS).
UNE-EN ISO/IEC 27001	Internacional	Seguridad de la información, ciberseguridad y protección de la privacidad.

REFERENCIA	CONTEXTO	DESCRIPCIÓN
		Sistemas de Gestión de Seguridad de la Información.
UNE-EN ISO/IEC 27002	Internacional	Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.
UNE-ISO 37301	Internacional	Compliance normativo.
Ley Orgánica 3/2018, de 5 de diciembre.	Nacional	Protección de Datos Personales y garantía de los derechos digitales.
El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.	Europeo	Protección de datos de carácter personal.
Documentos y Guías CCN-STIC	Nacional	Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.
Código Ético de SCAYLE	Interno	Por el que se rige la actuación de los miembros de SCAYLE.
Código Disciplinario de SCAYLE	Interno	Por el que se regulan las sanciones disciplinarias en el desarrollo de la actividad profesional de los empleados de SCAYLE.
Política de Seguridad de la información	Interno	Por el que se establecen las pautas, directrices y definiciones adoptadas por SCAYLE en el contexto de seguridad de la información.

6. NORMATIVA DE SEGURIDAD

6.1. Directrices generales de uso

Con carácter general, el uso de los sistemas de información de SCAYLE por parte de los usuarios atenderá invariablemente a los siguientes 4 criterios:

- Los usuarios **atenderán a las directrices de SCAYLE en el uso de los sistemas**. Se usarán solo para realizar las tareas indicadas y de la forma indicada. El uso de los principales sistemas está recogido en procedimientos específicos.
- Los usuarios **mantendrán la configuración de los sistemas a los que accedan tal cual la encontraron y no la modificarán en ningún caso**. Esta directriz se mantendrá incluso aunque los permisos del usuario se lo permitieran siempre y cuando no cuente con la indicación expresa del Responsable del Sistema.

- **Todo uso de los sistemas de información se hará**, salvo excepción, **conforme a las recomendaciones de uso del fabricante**. El Responsable del Sistema, previa valoración del impacto y de forma excepcional, puede establecer un uso no totalmente acorde a las recomendaciones del fabricante.
- **Seguridad proactiva.** Los usuarios finales forman parte de la cadena de la seguridad y de la eficiencia del servicio. Cuando observen comportamientos de los sistemas que consideren no habituales o anómalos, deben comunicarlo al Responsable del Sistema.

Como directriz genérica, los usuarios tienen permitido el uso de los sistemas de información de SCAYLE para la realización de su trabajo y/o para el cumplimiento de los objetivos para los cuales se le permitió originalmente el acceso

En este sentido, los usuarios deben cumplir, las siguientes directrices generales en el uso de medios personales:

- No está permitido conectar dispositivos que no estén autorizados a la red de SCAYLE.
- No se permite conectar a dispositivos autorizados otros dispositivos sin autorización expresa.
- No está permitido variar la ubicación física de los dispositivos asignados a una ubicación.
- No se permite utilizar, copiar o transmitir información contenida en los sistemas para un uso privado, desleal o ilícito.
- Se debe restringir a terceros el acceso a los archivos o ficheros titularidad de SCAYLE.

6.1.1. Propiedad y Uso de los Dispositivos

SCAYLE facilita a sus usuarios internos el equipamiento informático necesario para la realización de las tareas relacionadas con el puesto de trabajo, así como a los usuarios de los cursos de formación impartidos por la entidad. Este equipamiento es propiedad de SCAYLE y no se destina a uso personal. Como consecuencia de ello, SCAYLE se reserva el derecho de revisar, sin previo aviso, los equipos, uso de internet, teléfono y demás equipos que esté haciendo el usuario, en caso de que existan indicios de que se está llevando a cabo una utilización indebida.

Asimismo, SCAYLE se reserva el derecho de requerir la inmediata entrega del equipamiento en caso de que lo considere oportuno.

6.2. Directrices específicas de uso, usos permitidos y prohibidos

- Los sistemas de información de SCAYLE incluyen multitud de servicios y subsistemas que pueden ser usados por los usuarios para la ejecución de sus objetivos. Los más complejos disponen de procedimientos de seguridad a seguir aún más específicos.

- En todos ellos se deben seguir las siguientes directrices específicas de uso sin perjuicio de que procedimientos específicos establezcan protocolos más detallados.

Igualmente, se han previsto las siguientes pautas de actuación por parte del usuario:

- Los derechos de acceso a la información y a los Sistemas de Información que la tratan deberán siempre otorgarse en base a los principios de mínimo privilegio posible y necesidad de conocer.
- Cualquier información que el usuario almacene en los sistemas de SCAYLE debe cumplir con todos los requisitos legales aplicables.
- No se podrá acceder a los recursos informáticos y telemáticos de SCAYLE para desarrollar actividades que persigan o tengan como consecuencia:
    - El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones para usos no profesionales.
    - La degradación de los servicios.
    - Destrucción o modificación no autorizada de la información de manera premeditada.
    - La violación de la intimidad, el secreto de comunicaciones y del derecho a la protección de los datos personales.
    - El deterioro intencionado del trabajo de otras personas.
    - Dañar intencionadamente los recursos informáticos de SCAYLE
    - Incurrir en cualquier otra actividad ilícita del tipo que sea.
- No está permitido usar los privilegios de acceso para permitir el acceso a terceros ni a los servicios ni a las instalaciones.
- Todos los usuarios obtienen acceso a los sistemas y servicios de SCAYLE con uno o varios objetivos definidos (laboral o profesional, educativo, de investigación, etc.) y solo los utilizarán como medio para la consecución de esos objetivos.
- El servicio de correo electrónico no se usará para enviar nunca contenido inadecuado o para enviar correo a destinatarios desconocidos.
    - Se considera contenido inadecuado y su uso está terminantemente prohibido, aquel contenido ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad.
    - También lo es el software sin licencia, que vulnere los derechos de propiedad intelectual de los mismos, malware, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.
- No está permitido el acceso a las instalaciones de SCAYLE por parte de los usuarios excepto para el personal autorizado. Los proveedores y visitantes podrán acceder autorizados y acompañados por personal de SCAYLE.

6.3. Puesto de trabajo despejado y pantalla limpia

Para reducir los riesgos de acceso no autorizado, pérdida y daño de información en escritorios, pantallas y en otros lugares accesibles durante y fuera del horario laboral normal; los usuarios deben cumplir, las siguientes directrices:

- Conservar su escritorio libre de información propia de SCAYLE (papeles o unidades de almacenamiento externo) y conservar la pantalla del equipo de cómputo despejada de archivos office, pdf, entre otros, los cuales podrían ser copiados, utilizados o estar al alcance de terceros o por personal no autorizado.
- Bloquear la pantalla de su equipo de cómputo cuando no esté haciendo uso de este, o cuando por algún motivo deba ausentarse de su puesto de trabajo.
- Salir de todas las aplicaciones y apagar los equipos de cómputo y otros equipos de hardware que se encuentren en su puesto de trabajo al finalizar sus actividades diarias.
- Almacenar de forma segura documentos y soportes de almacenamiento extraíbles que contengan información sensible o crítica y, cuando ya no sea necesario, desecharlos utilizando mecanismos de eliminación seguros establecidos por SCAYLE.
- Después de imprimir documentos de carácter sensible o critica, evitar reutilizar y antes de reciclar destruir papel que contenga información sensible o critica.
- Proteger bajo llave la información sensible o critica (papeles o unidades de almacenamiento externo) en horario no hábil o cuando los puestos de trabajo se encuentren desatendidos
- Borrar información sensible o crítica de las pizarras y otros tipos de pantallas cuando ya no se necesario.

7. UTILIZACIÓN DE EQUIPOS INFORMÁTICOS Y DE COMUNICACIONES

SCAYLE facilita a los usuarios internos los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos que SCAYLE pone a disposición de los usuarios son propiedad de SCAYLE y deben utilizarse para el desarrollo de las funciones encomendadas, es decir, para fines profesionales. Cualquier uso de los recursos con fines distintos a los autorizados esta estrictamente prohibido.

En general, el ordenador personal (PC) será el recurso informático que permitirá el acceso de los usuarios a los sistemas de información y servicios informáticos de SCAYLE, constituyendo un elemento muy importante en la cadena de seguridad de los sistemas de información, razón por la que es necesario adoptar una serie de precauciones y establecer normas para su adecuada utilización.

7.1. Normas generales

- Los equipos informáticos serán asignados por el Área de Sistemas.
- Existirá un inventario actualizado de los equipos portátiles y móviles. El Área de Sistema será la unidad encargada de gestionar dicho inventario.
- A cada nuevo usuario que se incorpore a la organización y así lo precise, el área encargada le facilitara un ordenador personal debidamente configurado

y con acceso a los servicios y aplicaciones para el desempeño de sus competencias profesionales.

- Los equipos de trabajo, equipos portátiles y móviles propiedad de SCAYLE, deberán utilizarse únicamente para los fines institucionales autorizados, especialmente cuando se usen fuera de las instalaciones de SCAYLE, siendo estos una herramienta de apoyo a las competencias profesionales de los usuarios autorizados.
- Únicamente el personal autorizado por el Responsable del Sistema podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que deban repercutir en la Seguridad de los Sistemas de Información de SCAYLE.
- Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa del Responsable del Sistema. En todo caso, estas operaciones solo podrán realizarse por el personal de soporte técnico autorizado.
- Salvo autorización expresa del Responsable del Sistema, los usuarios por defecto no tendrán privilegio de administración sobre los equipos.
- Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitar únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizara completado el mantenimiento o una vez resueltos aquellos.
- Si el personal de soporte técnico detectase cualquier anomalía que indicará una utilización de los recursos contraria a la presente normativa, lo pondrá en conocimiento del Responsable del Sistema, que tomará las oportunas medidas correctoras y dará traslado de la incidencia al Responsable de Seguridad.
- Los ordenadores personales de la organización deberán mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.
- Los usuarios deben notificar al Responsable de Seguridad, a la mayor brevedad posible, cualquier comportamiento anómalo de su ordenador personal, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. Deberá comunicar también cualquier incidencia relacionada con la custodia, mantenimiento o reparación de los dispositivos al Área de Sistemas.
- Salvo aquellos ordenadores instalados en las zonas comunes de acceso a Internet, cada equipo se encuentra asignado a un usuario o grupo de usuarios concreto. Tales usuarios son responsables de su uso correcto.
- El usuario deberá participar en el cuidado y mantenimiento del equipo que tiene asignado, detectando la ausencia de cables y accesorios, y dando cuenta al Responsable del Sistema de tales circunstancias.
- El usuario deberá ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de disquetes, CDs/DVDs, memorias USB, mensajes de correo electrónico o instalación de programas descargados

desde Internet. Es imprescindible, por tanto, vigilar el uso responsable de los equipos para reducir este riesgo.

- El usuario será responsable de toda la información extraída fuera de la organización a través de dispositivos tales como memorias USB, CDs, DVDs, etc., que le hayan sido asignados. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate de información sensible, confidencial o protegida.
- El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata al Responsable del Sistema, al objeto de que le sean retirados los recursos informáticos que le hubieren sido asignados. Correlativamente, cuando los medios informáticos o de comunicaciones proporcionados por SCAYLE están asociados al desempeño de un determinado puesto o función, la persona que los tenga asignados tiene que devolverlos inmediatamente cuando finalice su vinculación con dicho puesto o función. Asimismo, durante periodos de baja laboral o inactividad prolongada, SCAYLE podrá requerir para la devolución de los equipos.
- En el caso de los dispositivos móviles que salgan de las instalaciones de SCAYLE, el usuario se hará responsable de su correcta custodia, evitando que los equipos queden fuera de su alcance o sin disponer de las medidas de seguridad necesarias para evitar el acceso por parte de terceros. Los usuarios de estos equipos son responsables de que no sean usados por terceras personas ajenas a SCAYLE o por personas no autorizadas para ello.
- No se podrán eliminar o deshabilitar las aplicaciones informáticas instaladas por el Responsable del Sistema, especialmente aquellas relacionadas con la seguridad.

7.2. Usos específicamente prohibidos

Están terminante prohibidos los siguientes comportamientos:

- **Está prohibido comer, beber o fumar junto a equipos o soportes informáticos.**
- Ejecución remota -salvo autorización- de archivos de tipo audiovisual (música, video, animaciones, etc).
- Utilización de cualquier tipo de software dañino.
- Utilización de programas que, por su naturaleza, hagan un uso abusivo de la red.
- Conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por SCAYLE, sin la previa autorización del Responsable de Seguridad.
- Utilización de conexiones y medios inalámbricos con tecnologías Wifi, Bluetooth o infrarrojos que no estén debidamente autorizados por el Responsable del Sistema.
- Utilización de dispositivos USB, teléfonos móviles u otros elementos, como acceso alternativo a Internet, salvo autorización expresa del Responsable del Sistema.
- Instalación y/o utilización de programas o contenidos que vulneren la legislación vigente en materia de Propiedad Intelectual. Este comportamiento estará sometido a las previsiones disciplinarias, administrativas, civiles o penales descritas en las leyes.

- Queda terminantemente prohibida, salvo previa autorización al usuario, la salida de equipos, soportes o documentos que contengan información propiedad de SCAYLE.
- Se prohíbe terminantemente la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito de SCAYLE de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la organización.
- No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa del Responsable del Sistema.
- Está prohibido el uso de dispositivos extraíbles para la salida de información propiedad de SCAYLE salvo autorizaciones que se prevean en la normativa y procedimientos de seguridad

7.3. Normas específicas para el almacenamiento de información

Con carácter general, la información almacenada de forma local en los ordenadores personales de los usuarios (disco duro local, por ejemplo) no será objeto de salvaguarda mediante ningún procedimiento corporativo de copia de seguridad. Por tanto, cuando tal almacenamiento este autorizado en las normas internas correspondientes, se recomienda a los usuarios la realización periódica de copias de seguridad, especialmente de la información importante para el desarrollo de la actividad profesional.

SCAYLE pone a disposición de los usuarios autorizados sistemas de almacenamiento de información para contener la información generada y salvaguardada por los usuarios desde sus unidades locales. Debe tenerse presente que tales unidades corporativas son un recurso limitado y compartidos por todos los usuarios, por lo que solo deberá salvaguardarse la información que se considere estrictamente necesaria.

No está permitido almacenar información personal privada, de cualquier naturaleza, en los recursos de almacenamiento compartidos o locales, salvo autorización previa del Responsable de la Información.

7.4. Normas específicas para equipos portátiles y móviles

- Los equipos portátiles y móviles serán asignados por el Área de Sistemas.
- Existirá un inventario actualizado de los equipos portátiles y móviles. El Área de Sistemas será la unidad encargada de gestionar dicho inventario.
- Este tipo de dispositivos estará bajo la custodia del usuario que los utilice o del responsable de la unidad. Ambos deberán adoptar las medidas necesarias para evitar daños o sustracción, así como el acceso a ellos por parte de personas no autorizadas.
- La sustracción de estos equipos se ha de poner inmediatamente en conocimiento del Responsable de seguridad y el Área de Sistemas para la

adopción de las medidas que correspondan y a efectos de baja en el inventario.

- Los equipos portátiles y móviles deberán utilizarse únicamente para fines institucionales y autorizados, especialmente cuando se usen fuera de las instalaciones de SCAYLE.
- Los usuarios de estos equipos se responsabilizarán de que no serán usados por terceras personas ajenas a SCAYLE o no autorizadas para ello.
- En general, los equipos portátiles no deberán conectarse directamente a redes públicas (Aeropuertos, cafés, centros comerciales, etc.). SCAYLE puede proporcionar accesos remotos autorizados y configurados por el Área de Sistemas a través de tarjetas móviles. Cuando este sea el caso, deberán realizar de forma obligatoria dicha conexión cuando requieran el acceso a Internet desde dichos equipos. En casos debidamente justificados y previamente autorizados por el Responsable del Sistema se podrá hacer uso de conexiones alternativas, observando estrictas medidas de seguridad en cuanto a la navegación en Internet y el resto de los preceptos de la presente Normativa General que resulten de aplicación.
- Los usuarios de equipos portátiles deberán realizar conexiones periódicas (al menos una vez por semana) a la red corporativa, según las instrucciones proporcionadas por el Área de Sistemas, para permitir la actualización de aplicaciones, sistema operativo, firmas de antivirus y demás medidas de seguridad. En su defecto, cada dos semanas, los equipos portátiles serán entregados al Área de Sistemas para la actualización de tal software.
- Cuando la tipología de la información tratada así lo requiera, los ordenadores portátiles afectados deberán tener cifrado el disco duro, disponer de software que garantice un arranque seguro, así como mecanismos de auditoría capaces de crear un registro por cada fichero extraído del sistema por cualquier medio (red, dispositivos extraíbles, impresoras, etc.).
- Como norma general, los equipos portátiles se configurarán por defecto con todos los canales, puertos y sistemas de comunicaciones de salida de información bloqueados (WiFi, Bluetooh, USB's, CD, DVD, tarjetas de red, etc.). Por petición justificada dirigida al Responsable del Sistema, se podrán habilitar algunas o todas las funciones de salida de información.
- Los usuarios no tendrán privilegio de administración sobre los equipos portátiles, teniendo prohibido realizar cualquier modificación hardware/software sobre los mismos. Corresponderá al Área de Sistemas llevar a cabo estas modificaciones.
- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, el usuario lo devolverá al Área de Sistemas, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a un nuevo usuario.

7.5. Normas específicas para memorias/lápices USB (pendrive)

- Con carácter general, el uso de memorias USB en SCAYLE no está autorizado. En su caso, la autorización deberá proporcionarla el Responsable del Sistema.
- Por razones de seguridad, únicamente se encuentran habilitados los medios de almacenamiento removibles propiedad de SCAYLE, los demás dispositivos ajenos a SCAYLE estarán deshabilitados. En caso de ser necesaria

su habilitación deberá justificarse por el usuario y requerirá la previa autorización del jefe de la unidad y el Responsable de Seguridad.

- En el caso de que a un usuario se le autorice el uso del interfaz USB de su puesto de trabajo, las memorias USB utilizadas serán las proporcionadas por SCAYLE, que serán conformes a las normas de seguridad de la organización. Estás memorias USB serán de uso exclusivo en los puestos de usuario de SCAYLE, no debiendo ser usados fuera de estos. Con el objetivo de preservar la confidencialidad de la información, deberán cifrarse los medios de almacenamiento que contengan información de uso interno y/o confidencial.
- Se recuerda que las memorias USB están destinadas a un uso exclusivamente profesional, como herramienta de transporte de ficheros, no como herramienta de almacenamiento. El Área de Sistemas podrá poner a disposición de los usuarios aplicaciones, servicios y sistemas de SCAYLE unidades de almacenamiento en red, que podrán usarse para tal propósito.
- La pérdida o sustracción de una memoria USB, con indicación de su contenido, deberá ponerse en conocimiento del Responsable de Seguridad y el Área de Sistemas, de forma inmediata.

7.6. Grabación de CDs y DVDs

- Con carácter general, el uso de equipos grabadores de CDs y DVDs en SCAYLE no está autorizado. En su caso, la autorización deberá proporcionarla el Responsable del Sistema.

- Por razones de seguridad, los equipos grabadores de CDs y DVDs de los puestos de trabajo estarán deshabilitados. En el caso de ser necesaria su habilitación, deberá justificarse por el usuario y requerirá la previa autorización del jefe de la unidad y por el Responsable del Sistema.

7.7. Copias de seguridad

- Mantener copias de seguridad es una cautela esencial de protección de la información.
- Los datos generados por el usuario en el desempeño de sus competencias profesionales deberán mantenerse en un repositorio único, en el sistema de almacenamiento de información proporcionado por SCAYLE.
- De forma periódica, se realizarán copias de seguridad, tanto completas como incrementales, de las unidades del sistema de almacenamiento de información de SCAYLE donde se almacene la información del usuario. En ningún caso se realizará copia de seguridad de la información almacenada de forma local en el puesto del usuario.

La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente. Para recuperar esta información el usuario habrá de dirigirse a la herramienta de gestión de servicios, gestionada por el Área de Sistemas.

7.8. Borrado y eliminación segura de soportes informáticos.

Las copias de seguridad o los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan información sensible, confidencial o protegida, deberán ser eliminados de forma segura para evitar accesos ulteriores a dicha información. En este sentido, el usuario deberá:

- Asegurarse del contenido de cualquier soporte antes de su eliminación (Área de Sistemas)
- Cuando contenga información sensible, confidencial o protegida, el soporte deberá borrarse o destruirse de forma segura según los procedimientos establecidos por SCAYLE.
- Cualquier petición de eliminación de soporte informático deberá ser autorizada expresamente por el Responsable de la Información, previa petición del jefe de la unidad. Esta petición debe dirigirse a través de la apertura de una incidencia a la herramienta de gestión de servicios gestionada por el Área de Sistemas que será el responsable de la destrucción o almacenamiento de los medios informáticos obsoletos.

7.9. Impresoras en red, fotocopiadoras y faxes

Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. En ningún caso el usuario podrá hacer uso de impresoras, fotocopiadoras o equipos de fax que no hayan sido proporcionados por SCAYLE y, en su consecuencia, estén debidamente inventariados.

Cuando se imprima documentación, deberá permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.

Conviene no olvidar tomar las originales de la fotocopiadora, una vez finalizado el proceso de copia. Si se encontrase documentación sensible, confidencial o protegida abandonada en una fotocopiadora o impresora, el usuario intentara localizar a su propietario para que este la recoja inmediatamente. En caso de desconocer a su propietario o no localizarlo, pondrá en conocimiento el incidente de seguridad al Responsable de Seguridad.

Los documentos que se envíen por fax deberán retirarse inmediatamente del equipo, de modo que nadie tenga acceso a su contenido si no se dispone de la autorización precisa.

7.10. Digitalización de documentos

Con carácter general, cuando se digitalicen documentos el usuario deberá ser especialmente cuidadoso con la selección del directorio compartido donde habrán de almacenarse las imágenes obtenidas, especialmente si contienen información sensible, confidencial o protegida.

Conviene no olvidar tomar los originales del escáner, una vez finalizado el proceso de digitalización. Si se encontrase documentación sensible, confidencial o protegida abandonada en un escáner, el usuario intentara localizar a su propietario para que este la recoja inmediatamente. En caso de desconocer a su propietario o no localizarlo, pondrá en conocimiento el incidente de seguridad al Responsable de Seguridad.

7.11. Cuidado y protección de la documentación impresa.

La documentación impresa que contenga datos sensibles, confidenciales o protegidos, debe ser especialmente resguardada, de forma que solo tenga acceso a ella el personal autorizado, debiendo ser recogida rápidamente de las impresoras y fotocopiadoras y ser custodiada en armarios bajo llave.

Cuando concluya la vida útil de los documentos impresos con información sensible, confidencial o protegida, deberán ser eliminados en las máquinas destructoras de SCAYLE, de forma que no sea recuperable la información que pudieran contener.

Si, una vez impresa, es necesario almacenar tal documentación, el usuario habrá de asegurarse de proteger adecuadamente y bajo llave aquellas copias que contengan información sensible, confidencial o protegida, o crítica para su trabajo.

Por razones ecológicas y de seguridad, antes de imprimir documentos, el usuario debe asegurarse de que es absolutamente necesario hacerlo.

7.12. Pizarras, rotafolios, pantallas, entre otros.

Cuando se hagan presentaciones, proyectos u otras actividades profesionales, antes de abandonar las salas o permitir que alguien ajeno entre, se deben limpiar adecuadamente las pizarras, rotafolios y demás elementos de las salas de reuniones o despachos, cuidando que no quede ningún tipo de información sensible que pudiera ser reutilizada. Si se utilizan medios de almacenamiento removibles, no se deben dejar conectados, esto aplica tanto en instalaciones internas propias como externas de SCAYLE.

7.13. Protección de la Propiedad Intelectual

Está estrictamente prohibida la ejecución de programas informáticos en los Sistemas de Información de SCAYLE sin la correspondiente licencia de uso. Los programas informáticos propiedad de SCAYLE o licenciados a SCAYLE están protegidos por la vigente legislación sobre Propiedad Intelectual y, por tanto, esta estrictamente prohibida su reproducción, modificación, cesión, transformación o comunicación, salvo que los términos del licenciamiento lo permitan y con la autorización previa del Responsable del Sistema.

Análogamente, está estrictamente prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier otro tipo de obra protegida por derechos de Propiedad Intelectual, sin la debida autorización del Responsable del Sistema.

7.14. Protección de la dignidad de las personas

Esta terminante prohibida toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.

En este sentido, dentro del sistema de gestión de compliance implementado en SCAYLE, se encuentra habilitado un Canal de denuncias, disponible en la página web de la Fundación, para la denuncia de este tipo de conductas. Sin perjuicio de la interposición de las acciones legales oportunas en su caso.

8. USO EFICIENTE DE EQUIPOS Y RECURSOS INFORMÁTICOS

Dentro de las medidas de austeridad y reducción del gasto de SCAYLE, se promueven las siguientes acciones para un uso más eficiente de los medios tecnológicos puestos a disposición de los usuarios:

- Apagar el PC (y la impresora local, en su caso), al finalizar la jornada laboral. Esta medida obedece tanto a razones de seguridad como de eficiencia energética.
- Imprimir únicamente aquellos documentos que sean estrictamente necesarios. La impresión se hará, preferiblemente, a doble cara y evitando siempre que sea posible, la impresión en color.
- Puesto que los recursos de almacenamiento en red son limitados y compartidos entre todos los usuarios, es preciso hacer un uso responsable de los mismos y almacenar únicamente aquella información que sea estrictamente necesaria.

9. INSTALACIÓN DE SOFTWARE

Únicamente el personal de soporte técnico autorizado por el Responsable del Sistema podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios.

Excepción a esta norma serán aquellas herramientas de uso común incluidas en el Catálogo de aplicaciones autorizadas de SCAYLE gestionado por el Área de Sistemas. Todo usuario podrá solicitar la inclusión de una aplicación en dicho Catálogo de aplicaciones autorizadas para su estudio por parte del Responsable del Sistema.
No se podrá instalar o utilizar software que no disponga de la licencia correspondiente o cuya utilización no sea conforme con la legislación vigente en materia de Propiedad Intelectual.

Se prohíbe terminantemente la reproducción, modificación, transformación, cesión, comunicación o uso fuera del ámbito de SCAYLE de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la organización.

En ningún caso se podrá eliminar o deshabilitar las aplicaciones informáticas instaladas por el Área de Sistemas, especialmente aquellas relacionadas con la seguridad.

10. ACCESO A LOS SISTEMAS DE INFORMACIÓN

Los datos gestionados por SCAYLE y tratados por cualquier Sistema de Información de SCAYLE deben tener asignado un responsable, que será el encargado de conceder, alterar o anular la autorización de acceso a dichos datos por parte de los usuarios.

El alta de los usuarios será comunicada inicialmente al Área Administrativa y posteriormente al Área de Sistemas. Para acceder a los recursos informáticos es necesario tener previamente una cuenta de usuario y estar dado de alta en los servidores del dominio. La autorización del acceso establecerá el perfil necesario con el que se configure las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar por el Área de Sistemas en caso de mala utilización.

Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.

Cuando un usuario deje de atender un PC durante cierto tiempo, es necesario bloquear la sesión o activar el salvapantallas, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivos de almacenamiento extraíble, entre otros; que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de terceros no autorizados. Por razones de seguridad, el PC de un usuario se bloqueará automáticamente tras un periodo de inactividad.

La baja de los usuarios será comunicada al Área Administrativa y al Área de Sistemas, para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo.

11. IDENTIFICACIÓN Y AUTENTICACIÓN

Los usuarios dispondrán de un identificador de usuario y una contraseña, tokens de seguridad o bien de una tarjeta de acceso o llave, para el ingreso a las dependencias y Sistemas de Información de SCAYLE, y son responsables de la custodia de estos y de toda actividad relacionada con el uso de su acceso autorizado. El nombre de usuario es único para cada persona en la organización, intransferible e independiente del PC, terminal, aplicación o Sistema de Información desde el que se realiza el acceso.

Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso o tarjeta criptográficas a otra persona, ni mantenerlas por escrito a la vista o alcance de terceros. El incumplimiento de este apartado se considerará un incidente de Seguridad y deberá notificarse de forma inmediata al Responsable de Seguridad.

Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.

Si un usuario tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe proceder inmediatamente a comunicar al Responsable de Seguridad la correspondiente incidencia de seguridad.

SCAYLE nunca solicitará al usuario sus credenciales de acceso (identificación de la cuenta y contraseña), por lo que si en un momento dado, un usuario recibiera una llamada telefónica solicitándole esta información. Nunca facilitará dichos datos y procederá a comunicar este hecho al Responsable de Seguridad de forma inmediata.

12. CONFIDENCIALIDAD DE LA INFORMACIÓN

Como medida de protección de la información propia, confiada o tratada por SCAYLE, está absolutamente prohibido el envío al exterior de información confidencial, electrónicamente, mediante soportes informáticos o por cualquier otro medio, que no hubiese sido previamente autorizado por el Responsable de Seguridad.

Todo el personal de la organización o ajeno a la misma que, por razón de su actividad profesional, hubiera tenido acceso a información gestionada por SCAYLE (tal como datos personales, documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.

En el caso de entrar en conocimiento de información que no sea de libre difusión, en cualquier tipo de soporte, deberá entenderse que dicho comportamiento es estrictamente temporal mientras dure la función encomendada, con la obligación de secreto o reserva indefinidas y sin que ello confiera derecho alguno de posesión, titularidad o copia de este. Asimismo, se deberán devolver los soportes de información utilizados inmediatamente después de la finalización de las tareas que hubieran originado su uso.

Los usuarios sólo podrán acceder a aquella información para la que posean las debidas y explícitas autorizaciones, en función de las labores que desempeñen, no pudiendo en ningún caso acceder a información perteneciente a otros usuarios o grupos de usuarios para los que no posea tal autorización.

Los derechos de acceso a la información y a los Sistemas de Información que la tratan deberán siempre otorgarse en base a los principios de mínimo privilegio posible y necesidad de conocer.

La información contenida en los Sistemas de Información de SCAYLE es propiedad de la Fundación Centro de Supercomputación de Castilla y León (SCAYLE), por lo que los usuarios deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros dicha información, salvo autorización expresa del Responsable de Seguridad.

Los soportes de información que vayan a ser reutilizados o causen baja deberán ser previamente tratados para eliminar permanentemente la información que pudieran contener, de manera que resulte imposible su recuperación. Estos soportes deberán entregarse al Responsable del Sistema.

Se evitará almacenar información sensible, confidencial o protegida en medios desatendidos (tales como CDs, DVDs, memorias USB, listados, etc.) o dejar visible tal información en la misma pantalla del ordenador.

Datos protegidos y datos de carácter personal: El Reglamento General de Protección de Datos 2016/679 (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos protegen los datos personales independientemente de la tecnología utilizada para su almacenamiento y/o tratamiento y se aplica tanto al tratamiento automatizado como manual, siempre que los datos se organicen con arreglo a criterios predeterminados (como el orden alfabético). Igualmente, no importa cómo se conservan los datos en todos estos casos, los datos personales están sujetos a los requisitos de protección establecidos en el RGPD.

Respecto al almacenamiento de información, los datos deberán estar en el espacio de red habilitado a fin de realizar copias de seguridad y proteger el acceso a personas no autorizadas.

Únicamente las personas autorizadas podrán introducir, modificar o anular datos o datos personales de los ficheros.

Los ficheros temporales que se generen deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación, y mientras estén vigentes, deberán estar almacenados en red.

12.1. Ficheros en papel

En relación con la documentación en soporte papel, el usuario deberá observar las siguientes diligencias respecto a la confidencialidad de la información, acceso autorizado, gestión de soportes y documentos y trabajo fuera de las instalaciones:

- Respecto a los archivos y dependencias, deberá haber una correcta custodia de llaves de acceso a locales y dependencias, así como a armarios y otros soportes con información.
- Deberán cerrarse con llave las puertas de despachos en casos de ausencias o a fin de evitar accesos no autorizados.
- El archivo de documentación se realizará siguiendo los criterios de la Organización.
- Los soportes que contengan información se archivarán en el lugar correspondiente, de modo que permitan una buena conservación, clasificación, acceso y uso de éstos.
- Cuando los documentos en soporte papel no estén almacenados, el usuario que los tenga a su cargo deberá custodiarlos e impedir el acceso por terceros no autorizados.
- El usuario debe asegurarse de que no hay impresos con datos personales en bandejas de fotocopiadoras, impresoras o faxes.
- En los traslados de documentación deberán adoptarse medidas para impedir el acceso o manipulación de la información, de forma que no se tenga acceso al contenido. Se mantendrán fuera del alcance de cualquier persona.
- La destrucción de papel deberá realizarse de forma segura y a través de los medios puestos a disposición por SCAYLE.

13. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER SECRETO

La información contenida en las bases de datos de la SCAYLE que comprenda datos de carácter personal está protegida por la normativa vigente, europea y nacional, en materia de Protección de Datos. Los Ficheros o Tratamientos de datos de carácter personal gestionados por SCAYLE han de adoptar las medidas de seguridad que se correspondan con las exigencias previstas o derivadas de la antedicha normativa.

Todo usuario (de SCAYLE o de terceras organizaciones) que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la SCAYLE.

14. TRATAMIENTO DE LA INFORMACIÓN

Toda la información contenida en los Sistemas de Información de SCAYLE o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones encomendadas a SCAYLE y a su personal.

Cualquier tratamiento en los Sistemas de Información de SCAYLE deberá ser conforme con la normativa vigente, especialmente con lo dispuesto en la normativa vigente europea y nacional, en materia de Protección de Datos.

Queda prohibido, asimismo, transmitir o alojar información sensible, confidencial o protegida propia de SCAYLE en servidores externos a SCAYLE salvo autorización expresa del Delegado de Protección de Datos, que comprobará la inexistencia de trabas legales para ello y verificará la suscripción de un contrato expreso entre la SCAYLE y la empresa responsable de la prestación del servicio, incluyendo los Acuerdos de Nivel de Servicio que procedan, el correspondiente Acuerdo de Confidencialidad, y siempre previo análisis de los riesgos asociados a tal externalización.

15. SALIDAS DE INFORMACIÓN

La salida de información de SCAYLE (en cualquier soporte o por cualquier medio de comunicación) deberá ser realizada exclusivamente por personal autorizado por el Responsable de Seguridad, previa autorización del jefe de la unidad, autorización que contemplará igualmente a la propia información que sale.

La salida de datos sensibles, confidenciales o protegidos requerirá su cifrado o la utilización de cualquier otro mecanismo que garantice que la información no será inteligible durante su remisión o transporte. Adicionalmente, si la información en cuestión contiene datos de carácter personal, se actuará conforme a lo dispuesto en la normativa vigente en materia de Protección de Datos.

Los usuarios se abstendrán de sacar al exterior cualquier información de SCAYLE en cualquier dispositivo (CDs, DVDs, memorias USB, ordenadores o dispositivos portátiles, etc.), salvo en los supuestos indicados en los puntos anteriores.

16. USO DEL CORREO ELECTRÓNICO CORPORATIVO

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los usuarios de SCAYLE, para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas.

Se trata de un recurso compartido por todos los usuarios de la organización, por lo que un uso indebido del mismo repercute de manera indirecta en el servicio ofrecido a todos.

Por ello, se dictan las siguientes normas de uso:

16.1. Normas generales

- Todos los usuarios que lo precisen para el desempeño de su actividad profesional, dispondrán de una cuenta de correo electrónico para el envío y recepción de mensajes internos y externos de la organización.
- Únicamente podrán utilizarse las herramientas y programas de correo electrónico suministrados, instalados y configurados por SCAYLE.
- El correo electrónico corporativo deberá utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal, quedando totalmente prohibido el uso privado del mismo.
- Se deberá notificar al Responsable de Seguridad cualquier tipo de anomalía detectada, así como los correos no deseados (spam) que se reciban, a fin de configurar adecuadamente las medidas de seguridad oportunas.
- Se deberá prestar especial atención a los ficheros adjuntos en los correos recibidos. No deben abrirse ni ejecutarse ficheros de fuentes no fiables, puesto que podrían contener virus o código malicioso. En caso de duda sobre la confiabilidad de los mismos, se deberá notificar esta circunstancia al Responsable de Seguridad.
- Para verificación y monitorización, los datos de conexión y tráfico se guardarán en un registro durante el tiempo que establezca la normativa vigente en cada supuesto. En ningún caso esta retención de datos afectará al secreto de las comunicaciones.

16.2. Usos especialmente prohibidos

Las siguientes actuaciones están explícita y especialmente prohibidas:

- El envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, que contengan programas informáticos (software) sin licencia, que vulneren los derechos de propiedad intelectual de los mismos, de alerta de virus falsos o difusión de virus reales y código malicioso, o cualquier otro tipo de contenidos que puedan perjudicar a los usuarios, identidad e imagen corporativa y a los propios sistemas de información de la organización.
- El acceso a un buzón de correo electrónico distinto del propio y el envío de correos electrónicos con usuarios distintos del propio.
- Está terminantemente prohibido suplantar la identidad de un usuario de internet, correo electrónico o cualquier otra herramienta colaborativa.
- La difusión de la cuenta de correo del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional del usuario.
- Responder mensajes de los que se tengan sospechas sobre su autenticidad, confiabilidad y contenido, o mensajes que contengan publicidad no deseada.
- La utilización del correo corporativo como medio para recoger correo de buzones que no pertenezcan a SCAYLE o el reenvío automático del correo corporativo a buzones ajenos a la organización. Para ello se necesitará la autorización expresa del Responsable de Seguridad.

Nota: SCAYLE podrá revisar y controlar el uso correcto del correo electrónico. Igualmente, durante periodos de ausencia, baja temporal o definitiva, se podrá

consultar el buzón de correo o redireccionar su cuenta con la finalidad de continuar con el desarrollo de la actividad de la Organización.

16.3. Recomendaciones adicionales

- Se debe asegurar que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.
- Evitar en la medida de lo posible el uso ineficiente de los envíos de correo. Para ello se deben agrupar los envíos a múltiples destinatarios en un solo mensaje, se debe evitar la incorporación de firmas escaneadas, imágenes y fondos como formato habitual de los correos teniendo en cuenta que incrementan innecesariamente el tamaño y volumen de estos.
- Los buzones de correo se configuran con un tamaño de almacenamiento limitado a 25GB. El sistema indicará cuándo se encuentra al límite de su capacidad, tras el cual no se permitirá enviar y recibir correos.

17. USO DE LA CONEXIÓN A INTERNET

El acceso corporativo a Internet es un recurso centralizado que SCAYLE pone a disposición de los usuarios como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional.

SCAYLE velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso.

17.1. Normas generales

- **Usar Internet para fines profesionales**. Internet es una herramienta más de las utilizadas por los usuarios de **SCAYLE**. Por ello, debe usarse de manera responsable y exclusivamente para fines profesionales (docencia, investigación, formación y uso administrativo). Si en algún caso fuese necesario realizar un uso personal (Por ejemplo, acceso a nóminas o gestión de vacaciones), se deberá utilizar un navegador web diferente al utilizado habitualmente para uso profesional, de forma que se separen las cookies almacenadas y se evite la contaminación entre uso personal y uso organizativo.

- **No visitar páginas de contenido poco ético, ofensivo o ilegal.** No está permitido el acceso a páginas cuyo contenido pueda resultar ofensivo o atentar contra la dignidad humana. Análogamente, no se permite el acceso a páginas de contenido no adecuado, ilegal o poco ético.

- **No visitar páginas no fiables o sospechosas.** Para evitar posibles incidentes de seguridad, es aconsejable no visitar páginas que se consideren sospechosas de contener código malicioso.

- **Cuidar la información que se publica en Internet.** No se debe proporcionar información sobre la organización en foros, chats, etc., ya que podría ser utilizada de forma fraudulenta. En este sentido, está prohibido difundir sin

autorización cualquier tipo de información no pública sobre el funcionamiento interno de **SCAYLE**, sus recursos, estructura, etc.

- **Observar las restricciones legales que sean de aplicación.** Antes de utilizar una información obtenida de Internet, los usuarios deberán comprobar en qué medida se halla sujeta a los derechos derivados de la Propiedad Intelectual o Industrial.
- **Realizar descargas sólo si se tiene autorización.** Las descargas indiscriminadas o sin autorización son uno de los orígenes más usuales de infección por código malicioso. Aunque **SCAYLE** decida no limitar técnicamente la capacidad para descargar archivos de audio o vídeo, los usuarios deberán tener en consideración que la descarga de estos archivos puede ir en detrimento del rendimiento de los recursos informáticos y, por ello, limitarán su descarga y reproducción al ámbito estrictamente profesional.
- **No descargar código o programas no confiables.** Es necesario asegurar la confiabilidad del sitio desde el cual se descargan los programas, utilizando siempre las páginas oficiales. Además, es necesario comprobar si es preciso el uso de licencia para utilizar las aplicaciones descargadas. Conviene que tales actividades sean acometidas, de manera exclusiva, por el Servicio de Tecnologías de la Información y las Comunicaciones (STIC).
- **Asegurar la autenticidad de la página visitada.** Cuando se vayan a realizar intercambios de información o transacciones es importante asegurar que la página que se visita es realmente la que dice ser. Es recomendable acceder a las páginas escribiendo y comprobando la dirección en la barra de direcciones del navegador y no a través de vínculos externos. Muchas suplantaciones de páginas Web muestran una página que es virtualmente idéntica a la página conocida por el usuario, incluso evidenciando un falso nombre en la barra de direcciones. Cuando la página web se encuentre autenticada mediante certificado digital, el usuario verificará su autenticidad.
- **Comprobar la seguridad de la conexión.** En general, la información transmitida por Internet no circula de manera cifrada. Sin embargo, en la transmisión de información sensible, confidencial o protegida es importante asegurar su cifrado. Una manera de asegurar la confidencialidad es comprobar que se utiliza protocolo HTTPS en la comunicación en vez del protocolo estándar HTTP (examinando la barra de direcciones). También debería aparecer un icono representando un candado en la barra del navegador. A través de dicho candado se puede obtener información sobre el certificado digital de identidad del sitio web visitado.
- **Cerrar las sesiones al terminar la conexión.** Es muy conveniente cerrar las sesiones al terminar la conexión o el intercambio de información (siempre que se haya autenticado en la página web), ya que en muchas ocasiones la conexión permanece abierta por defecto y no es suficiente con cerrar el navegador. Esto puede hacer que otros usuarios tengan acceso a las cuentas de los usuarios que no hubieren cerrado correctamente las sesiones. La mayoría de los sitios web disponen de una opción de "desconexión", "logout" o similar que conviene utilizar.

- **Utilizar herramientas contra código dañino.** El volumen de código dañino que circula en el ciberespacio es muy elevado y presenta multitud de aspectos diferentes. Por tanto, es necesario disponer del adecuado abanico de herramientas que permitan una adecuada protección. El uso de un antivirus permanentemente actualizado es la primera medida de protección contra este tipo de ataques. Además de ello, es necesario configurar y usar adecuadamente cortafuegos, software específico contra programas espía (spyware), etc.
- **Mantener actualizado el navegador y las herramientas de seguridad.** Es imprescindible actualizar las herramientas de acceso a Internet (navegadores) y de seguridad (antivirus, cortafuegos, etc.) a las últimas versiones estables, siempre de conformidad con lo indicado y aprobado por el STIC. Puesto que el código dañino se genera incesantemente, es muy importante actualizar las firmas de virus con la mayor frecuencia posible. Los sistemas deben estar configurados para realizar esta tarea de forma automática. Asimismo, es muy importante informar sobre cualquier problema que se detecte en este proceso.
- **Utilizar los niveles de seguridad del navegador.** Los navegadores Web permiten configuraciones con diferentes niveles de seguridad. Lo idóneo es mantener el nivel de seguridad "alto", no siendo recomendable utilizar niveles por debajo de "medio". Esto puede hacerse usando las herramientas disponibles en el navegador.
- **Desactivar las cookies.** Las cookies son pequeños programas fragmentos de texto que emplean los servidores Web para almacenar y recuperar información acerca de sus visitantes (Por ejemplo, quién, cuándo y desde dónde se ha conectado un usuario). Estos programas fragmentos de texto se almacenan en el ordenador del usuario al visitar una página Web, pudiendo ser desactivados usando las herramientas disponibles en el navegador.
- **Eliminar la información privada.** Los navegadores Web almacenan información privada durante su utilización, tal como el historial de navegación, cookies aceptadas, contraseñas, etc., información a la que podría acceder un atacante que se hubiera introducido en el sistema. Por tanto, es recomendable borrar esta información de manera periódica, usando las herramientas disponibles en el navegador.
- **No instalar complementos desconocidos.** Cuando se cargan ciertas páginas web, se muestra un mensaje comunicando la necesidad de instalar en el ordenador del usuario un complemento (plug-in, add-on, etc.) para poder acceder al contenido. Es muy recomendable analizar primero la conveniencia de instalar tal complemento y hacerlo, en cualquier caso, siempre desde la página del distribuidor o proveedor oficial del mismo.
- **Limitar y vigilar la ejecución de Applets y Scripts.** Los scripts son un conjunto de instrucciones que permiten la automatización de tareas. Los applets son pequeñas aplicaciones (componentes de aplicaciones) que se ejecutan en el contexto del navegador Web. A pesar de que, en general, resultan útiles, pueden ser usados para ejecutar código malicioso y, por tanto, es recomendable limitar su ejecución.

17.2. Usos específicamente prohibidos

Quedan prohibidas las siguientes actuaciones:

- Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos de SCAYLE, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.
- Queda expresamente prohibida la visualización de material con contenido sexual, obsceno, ofensivo, racista o que pueda ser considerado ilícito, a través de la red corporativa o servicios de internet de SCAYLE.
- Los logos, marcas y demás signos distintivos de SCAYLE no podrán ser utilizados por el usuario en Internet, salvo que se trate de alguna actividad desarrollada en representación de SCAYLE y se encuentre autorizada.
- La descarga de programas informáticos sin la autorización previa del Responsable del Sistema, o ficheros con contenido dañino, que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.
- 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 para la descarga masiva de archivos, programas u otro tipo de contenido que no esté expresamente autorizado por el Responsable del Sistema.
- Está prohibido el uso de sistemas de mensajería instantánea o chat en tiempo real (salvo que se utilice para la comunicación con clientes, proveedores o empleados de SCAYLE, su uso se ajuste a una finalidad productiva y laboral y haya sido previamente autorizado por el Responsable de Seguridad de SCAYLE).
- Queda prohibido el uso y la instalación de programas que permitan el acceso a redes P2P, así como cualquier otro tipo de acceso a entornos o plataformas que permitan el intercambio de ficheros sin la previa y expresa autorización del Responsable de Seguridad. Este tipo de programas puede ayudar a superar los sistemas de defensa ante accesos no autorizados y son un canal de virus y programas espía.
- No se podrá conectar en la red de comunicaciones corporativa ningún dispositivo distinto de los admitidos, habilitados y configurados por SCAYLE, salvo autorización previa del Responsable de Seguridad.

Nota: SCAYLE podrá controlar el uso de acceso a internet proporcionado. Para ello se seguirá un sistema basado en el control de recursos visitados, almacenamiento y recursos que se generen.

18. GESTIÓN DE CUENTAS DE USUARIO

El alta de los usuarios será comunicada inicialmente al Área Administrativa y posteriormente al Área de Sistemas. Si en el proceso de solicitud de cuenta de usuario, el solicitante no remite el modelo de declaración de usuario (aceptación de cumplimento de la presente Normativa) debidamente cumplimentado en un plazo inferior a 15 días hábiles, se tomará por desestimada dicha solicitud, con lo cual el Área Administrativa notificará al usuario y archivará la petición. En ese caso el usuario deberá realizar nuevamente el proceso de solicitud de creación de cuenta.

Para acceder a los recursos informáticos es necesario tener previamente una cuenta de usuario y estar dado de alta en los sistemas de información. La autorización del acceso establecerá el perfil necesario con el que se configure las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

Transcurridos **180 días** desde el alta de su cuenta o desde el último cambio de contraseña, el usuario deberá **cambiar la contraseña** de su cuenta de SCAYLE. Habrá recibido un aviso por correo con 10 días de antelación. Por tanto, las contraseñas **caducan cada 180 días máximo**.

Pasados **90 días** desde la caducidad de la contraseña, si el usuario **no ha cambiado la contraseña** de su cuenta, esta será bloqueada automáticamente. El **bloqueo** de la cuenta será comunicado a través de un email a la dirección de correo electrónico que tiene como contacto y copiando en el mail a las Áreas Técnica y Administrativa de SCAYLE.

A **los 30 días desde el bloqueo** de la cuenta, si esta no ha sido desbloqueada se procederá a dar de **baja** automáticamente la cuenta, notificando dicha baja a través de un email a la dirección de correo electrónico que tiene como contacto la cuenta y copiando en el mail a las Áreas Técnica y Administrativa de SCAYLE.

El Área Administrativa activará el procedimiento de baja de usuario descrito en **el procedimiento de gestión de usuarios,** lo cual implica también a la facturación.

18.1. Gestión de las contraseñas

- El usuario se compromete a mantener las contraseñas en secreto. No deben compartirse con nadie.
- Preferiblemente, las contraseñas iniciales deben ser entregadas a través de algún medio que no permita su acceso por personas no autorizadas.
- Como norma general no deben ser incluidas en correos electrónicos o en otros medios de comunicación electrónica, ni comunicadas por teléfono.
- En el caso de enviarlas por medios telemáticos (correo electrónico, SMS, etc.) o en un soporte, se enviarán separadas del identificador.
- Las contraseñas iniciales deben ser generadas automáticamente y se cambiarán antes del primer acceso a los sistemas.
- Los salvapantallas deben tener activada la protección por contraseña, bloqueándose tras un periodo de inactividad.
- No se deben escribir o almacenar contraseñas en texto claro o en formas fácilmente reversibles.
- Adicionalmente, deberán modificarse siempre que se sospeche que está comprometida a través de los procedimientos establecidos.

19. INCIDENTES DE SEGURIDAD

Cuando un usuario detecte cualquier anomalía o incidente de seguridad que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información SCAYLE o su imagen, deberá comunicarlo inmediatamente a la entidad, que dejará debidamente constancia de ello y, si es posible, comunicará la situación.

Todo usuario está obligado a notificar los incumplimientos de la presente normativa que detecte, así como cualquier tipo de incidencia, evento o circunstancia que ponga, o pueda poner, en peligro la seguridad de los datos personales y resto de información incorporados a nuestros ficheros.

La notificación se realizará mediante la cuenta de correo **seguridad@scayle.es** de SCAYLE, debiendo facilitar al menos la siguiente información sobre la incidencia detectada:

- Descripción del hecho o circunstancia que motiva la incidencia.
- Fecha y hora en la que se produjo o se detectó.
- Usuario que notifica la incidencia.

El Departamento Técnico –Responsable de Seguridad, será el responsable de la tramitación de la incidencia que quedará registrada en la aplicación informática empleada al efecto.

El tramitador de la incidencia deberá dejar constancia al menos de los efectos que puedan derivarse de esta incidencia y de las medidas correctoras que deban aplicarse para su subsanación. Si dentro de las medidas correctoras que debieran aplicarse para la subsanación de la incidencia, se incluyeran medidas relativas a la restauración de archivos desde las copias de respaldo o incluso la introducción manual de registros en programas o bases de datos, éstas deberán ser expresamente autorizadas por el Responsable de Seguridad.

A continuación, se exponen algunos ejemplos de incidencias o eventos a notificar:

- Detección de virus.
- Pérdida de equipos o soportes con datos personales.
- Detección de accesos no autorizados a información con datos personales.
- Detección de contraseñas no confidenciales.
- Detección de nombres de usuario compartidos.
- Salidas de soportes con datos personales no autorizadas.
- Utilización de soportes no autorizados o de forma contraria a las normas de SCAYLE.
- Detección de documentos con datos personales abandonados o destruidos de forma incorrecta.
- Existencia de archivos con documentos que contienen datos personales en armarios o cajones no cerrados.
- Documentos con datos personales olvidados en bandejas de impresión.
- Pérdida o robo de documentos con datos personales, etc.

20. USO ABUSIVO DE LOS SISTEMAS DE INFORMACIÓN

El uso de Internet, del correo electrónico y el acceso al resto de los servicios y sistemas de la SCAYLE estará debidamente controlado para todos los usuarios. Si se hiciese un uso abusivo o inapropiado de estos servicios, SCAYLE podrá adoptar las medidas disciplinarias que considere oportunas, sin perjuicio de las acciones civiles o penales a las que hubiere lugar.

Con carácter general, se enumeran seguidamente un conjunto de acciones que se consideran uso abusivo de los sistemas de información de SCAYLE.

20.1. Uso abusivo del acceso a Internet

- Acceso a otras redes, con el propósito de violar su integridad o seguridad.
- Acceso a los contenidos no relacionados con los cometidos profesionales del usuario, tales como:
    - Acceder, recuperar o visualizar textos o gráficos que excedan los límites de la ética.
    - Almacenar en la estación de trabajo del usuario o en los servidores de SCAYLE archivos personales.
    - Utilizar el acceso a Internet para el uso de mensajería instantánea (no autorizada.)
    - Transferencia de ficheros no relativa a las actividades profesionales del usuario (tales como juegos, ficheros de sonido, fotos, videos, películas, plataformas de streaming, etc.)
    - Realizar cualquier actividad de promoción de intereses personales.
- Publicación o envío de información no solicitada.
- Publicación o envío de información sensible, confidencial, protegida o propiedad de SCAYLE, a personas, empresas o sistemas de información externos no autorizados. En este sentido, los usuarios se comprometen a garantizar la privacidad de estos datos y contraseñas de acceso, así como evitar la difusión de estos.
- Publicación o envío de mensajes a través de Internet que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del servicio de Internet de manera ilegal o infringiendo cualquier norma interna que pudiera resultar de aplicación.
- Empleo de utilizades de intercambio de información en Internet (tales como redes P2P)
- Uso de Internet para propósitos que puedan influir negativamente en la imagen de SCAYLE, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.

20.2. Uso abusivo del correo electrónico corporativo.

- Utilizar el correo electrónico para fines distintos a los derivados de las actividades profesionales del usuario, específicamente:
    - Intercambiar contenidos (textos o gráficos) que excedan los límites de la ética.
    - Transparencia de ficheros ajena a las actividades profesionales del usuario (por ejemplo: software sin licencia, ficheros de sonido, fotos y videos, gráficos, virus, código malicioso, etc.)
    - Realizar cualquier actividad de promoción de intereses personales.
    - Usar cualquier cuenta de correo de SCAYLE para enviar mensajes o castas en cadena y/o correos basura o spam (correo electrónico no solicitado)
- Usar cualquier cuenta de correo de SCAYLE para enviar mensajes que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del correo electrónico de manera ilegal o infringiendo cualquier norma que pudiera resultar de aplicación.
- Revelar a terceros el contenido de cualquier dato reservado o confidencial propiedad de SCAYLE o de terceros, salvo que tal actuación fuera realizada

en cumplimiento de fines estrictamente profesionales con el previo consentimiento de los afectados.

- Utilizar para propósitos que puedan influir negativamente en la imagen de SCAYLE, de sus representantes o de los organismo públicos o privados con los que se mantiene relación.

20.3. Uso abusivo de otros servicios y sistemas de SCAYLE

- Acceso a servicios y/o contenidos de SCAYLE con el propósito de violar su integridad o seguridad.
- De forma general, realizar actividades no relacionadas con las tareas profesionales del usuario, tales como:
  - Acceder, recuperar, o visualizar textos o gráficos que excedan los límites de la ética.
  - Almacenar archivos personales en la estación de trabajo o en los servidores de SCAYLE.
  - El uso de mensajería instantánea (sin autorización).
  - Transferencia de ficheros entre usuarios de SCAYLE no relativa a las actividades profesionales.
  - Realizar cualquier actividad de promoción de intereses personales.
- Uso de cualquier servicio de SCAYLE para:
  - La publicación o envío de información no solicitada.
  - La publicación o envío de información confidencial, propiedad de SCAYLE, a personas, empresas o sistemas de información externos no autorizados. Los usuarios se comprometen a garantizar la privacidad de estos datos y contraseñas de acceso, así como evitar la difusión de estos.
  - El uso de los servicios de SCAYLE para propósitos que puedan influir negativamente en la imagen de SCAYLE, de sus representantes o de los organismos públicos o privados con los que se mantiene relación.
  - El envío de mensajes que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del correo electrónico de manera ilegal o infringiendo cualquier norma que pudiera resultar de aplicación.
- Comunicación a terceros del contenido de cualquier dato reservado o confidencial propiedad de SCAYLE o de terceros, salvo que tal actuación fuera realizada en cumplimiento de fines estrictamente profesionales con el previo consentimiento de los afectados.

Las acciones realizadas desde una cuenta de usuario o desde una cuenta de correo electrónico de usuario son responsabilidad de su titular.

SCAYLE implantara los sistemas de protección de acceso a los sistemas que considere necesario, para evitar que se produzcan incidentes relacionados con el abuso de estos servicios.

21. COMPROMISOS DE LOS USUARIOS

Es responsabilidad directa del usuario:

a) Custodiar las credenciales que se le proporcionen y seguir todas las recomendaciones de seguridad establecidas por SCAYLE, para que garantizar que aquellas no puedan ser utilizadas por terceros. Deberá cerrar su cuenta al terminar la sesión o bloquear el equipo cuando lo deje desatendido.

b) En el caso de que su equipo contenga información sensible, confidencial o protegida, esta deberá cumplir todos los requisitos legales aplicables y las medidas de protección que la normativa de SCAYLE establezca al respecto.

c) Garantizar la disponibilidad de toda la información importante para SCAYLE alojada en el equipo del usuario – si no residiera en los servidores corporativos -, mediante la realización de copias de seguridad periódicas.

Además de lo anterior, no se podrá acceder a los recursos informáticos y telemáticos de SCAYLE para desarrollar actividades que persigan o tengan como consecuencia:

a) El uso intensivo de recursos de proceso, memoria, almacenamiento o comunicaciones, para usos no profesionales.
b) La degradación de los servicios.
c) La destrucción o modificación no autorizada de la información, de manera premeditada.
d) La violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.
e) El deterioro intencionado del trabajo de otras personas.
f) El uso de los sistemas de información para fines ajenos a los de SCAYLE, salvo aquellas excepciones que contempla la Normativa.
g) Dañar intencionadamente los recursos informáticos de SCAYLE o de otras Instituciones.
h) Incurrir en cualquier otra actividad ilícita, del tipo que sea.

22. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

SCYALE, por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

a) Revisará el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
b) Monitorizará los accesos a la información contenida en sus sistemas.
c) Auditará la seguridad de las credenciales y aplicaciones.
d) Monitorizará los servicios de Internet, correo electrónico, sistemas de información y otras herramientas de colaboración.

SCAYLE llevará acabo esta actividad de monitorización de manera proporcional al riesgo, con las cautelas legales pertinentes y las señaladas en la jurisprudencia y con observancia de los derechos de los usuarios.

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se reestablecerá cuando la causa de su inseguridad o degradación desaparezca. El Responsable de Seguridad, con la colaboración de las restantes unidades de SCAYLE, velará por el cumplimiento de la presente Normativa General e informará sobre los incumplimientos o deficiencias de seguridad observados, al objeto de que se tomen las medidas oportunas.

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 dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como el tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar al Responsable del Sistema sobre usos prolongados e indebidos del servicio.

23. INCUMPLIMIENTO DE LA NORMATIVA

Todos los usuarios de los servicios de información de SCAYLE, sin excepción, están obligados a cumplir lo prescrito en la presente Normativa de Seguridad.

En el supuesto de que un usuario no observe algunos de los preceptos señalados en la presente Normativa General, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.

- Todos los usuarios de los sistemas de SCAYLE están obligados al cumplimiento de la normativa.
- Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.
- SCAYLE se reserva el derecho a revisar, sin previo aviso, los equipos y el uso de internet y de otros dispositivos por parte del usuario, en caso de indicios de utilización indebida.
- De este modo el usuario queda informado de que el resultado de los controles llevados a cabo puede provocar el inicio de las actuaciones disciplinarias necesarias en el marco de la legislación vigente.
- Cuando un usuario incumple la normativa de seguridad, se abrirá un proceso de análisis dirigido por el Responsable de Seguridad y encargado de establecer lo ocurrido y su nivel de impacto en la seguridad e integridad del sistema.
    - **Usuarios que no sean empleados de SCAYLE**: el Responsable de Seguridad elevará las conclusiones de su análisis al Comité de Seguridad, que será el encargado de decidir las **consecuencias para el usuario**. Esto puede ir desde el apercibimiento hasta la suspensión temporal o definitiva de su cuenta.
    - **Usuarios que sean empleados de SCAYLE:** el Responsable de Seguridad elevará las conclusiones a la Dirección General de SCAYLE, que será el encargado de decidir las consecuencias para el usuario. El resto del Comité de Seguridad actuará como órgano consejero. Las consecuencias pueden ir desde el apercibimiento, sanciones disciplinarias, o hasta las

que recoja la legislación laboral, civil y/penal ante un incumplimiento de contrato.
    - En ambos casos, todo uso inadecuado o incumplimiento de la normativa que atente contra la legislación vigente o contra los intereses de SCAYLE, será denunciado ante las autoridades competentes.

El usuario está obligado a:

- Notificar los incumplimientos de la presente normativa que detecte.
- Cualquier tipo de incidencia, brecha en la seguridad, evento o circunstancia que ponga o pueda poner en peligro la seguridad, disponibilidad o integridad de los sistemas de información de SCAYLE.
- El usuario deberá notificar esta circunstancia a través del sistema de gestión de tickets de SCAYLE o mediante la cuenta de correo **seguridad@scayle.es** de SCAYLE, debiendo facilitar al menos la siguiente información sobre la incidencia detectada:
    - Descripción del hecho o circunstancia que motiva la incidencia.
    - Fecha y hora en la que se produjo o se detectó.
    - Usuario que notifica la incidencia.

24. ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO (DECLARACIÓN DE USUARIO DE RECURSOS INFORMÁTICOS)

Todos los usuarios de los servicios de información de SCAYLE, sin excepción, deberán firmar la declaración de usuario, comprometiéndose con esta Normativa de Seguridad. Se mantendrá un registro con las declaraciones firmadas por todos los usuarios. Dicho registro será custodiado por el Área encargada en formato papel o electrónicamente.

25. ANEXOS

- SGSI-NOR01-A1: Normativa de Seguridad Anexo I Modelo declaración de responsabilidad de usuarios.