Código de conducta y buenas prácticas en materia de seguridad de la información y protección de datos para los usuarios de sistemas de información de la Gerencia Regional de Salud de Castilla y León

Oficina de Seguridad de la Información
11 de septiembre de 2023

USO INTERNO

Historia del documento			
Versión: **v1.0**	**Descripción: Código de conducta y buenas prácticas en materia de seguridad de la información y protección de datos para los usuarios de sistemas de información de la Gerencia Regional de Salud de Castilla y León**		
	Elaborado por:	Oficina de Seguridad de la Información	*Fecha*: 11/09/2023
	Validado por:	Responsable de la seguridad de la GRS	*Fecha*: 20/09/2023
	Aprobado por:	Comité de Seguridad de la Información	*Fecha*: 26/10/2023

Contenido

1 INTRODUCCIÓN

El uso del equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización del sector público. Estos medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para desempeñar su actividad profesional, razón por la cual compete a la Gerencia Regional de Salud de Castilla y León (en adelante, GRS), establecer las normas, las condiciones y las responsabilidades bajo las que se deben usar tales recursos tecnológicos.

Los usuarios deben estar formados y concienciados en materia de seguridad de la información y protección de datos, y usar estos recursos de manera que se preserve siempre la seguridad de la información manejada y de los servicios prestados.

En materia de protección de datos, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD), y la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDGDD), requieren que los responsables de tratamiento, a efectos de garantizar el principio de responsabilidad proactiva, determinen y apliquen las medidas técnicas y organizativas apropiadas al nivel de riesgo, para garantizar la seguridad de los datos, la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, la destrucción o el daño accidental, y acreditar que se cumple con el RGPD, la LOPDGDD, las normas que la desarrollan y la propia legislación sectorial aplicable.

En materia de seguridad de la información, el Real decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (en adelante, ENS), establece la necesidad de aplicar medidas de seguridad en el ámbito de protección de la información y de las comunicaciones, para proteger, en último término, tanto los propios sistemas de información, como la información procesada por estos.

Estos requerimientos se refuerzan con la obligación de garantizar la protección de los datos clínicos, derivada de aplicar la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que recoge diversas previsiones con la finalidad de proteger la confidencialidad y la intimidad relativas a la información relacionada con la salud de la ciudadanía.

Para dar cumplimiento a la normativa en materia de protección de datos y seguridad de la información, se hace necesario por parte de la GRS, incorporar al uso de las tecnologías de la información y de las comunicaciones, aquellas actuaciones que permitan garantizar un entorno seguro para el tratamiento de los datos y que optimicen el uso de los recursos disponibles en la prestación de los servicios sanitarios.

En este sentido, la GRS ha desarrollado su propia Política de Seguridad de la Información y Protección de Datos (también PSIPD), aprobada mediante el Decreto 14/2023, de 21 de agosto, y que establece los principios fundamentales, la estructura organizativa encargada de la gestión de la PSIPD, el desarrollo y las directrices para gestionar las medidas de seguridad que garanticen el cumplimiento de la normativa vigente y el uso seguro y eficiente de los recursos en la prestación de los servicios sanitarios.

El presente documento, que forma parte del marco normativo de seguridad y protección de datos previsto por la PSIPD, detalla las medidas de seguridad orientadas a los usuarios, a fin de garantizar la seguridad de la información y la protección de los datos personales tratados.

1.1 Objeto y alcance

El objeto del presente documento es establecer un código de conducta y buenas prácticas para los usuarios de recursos tecnológicos de la GRS, a fin de optimizar el uso de recursos y mantener la seguridad, la confidencialidad, la disponibilidad y la integridad de sus datos, todo ello sin perjuicio de que a su vez se deba cumplir con la normativa vigente, con lo dispuesto en la PSIPD y demás normativa aplicable.

El personal de la GRS en el cumplimiento de sus funciones, así como el personal de las empresas externas, públicas y privadas, que, por razón de la prestación de un servicio determinado, tengan acceso a los datos y/o sistemas de información de la GRS, deben conocer y aplicar los requisitos y las instrucciones de este código de conducta y buenas prácticas.

El código de conducta y buenas prácticas es aplicable para el uso de todos los recursos equipamiento físico, equipamiento lógico, servicios e información— usados por el personal de la GRS así como por el personal de las empresas externas, públicas y privadas, para desempeñar sus funciones, en todas las fases del ciclo de vida de los datos (generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción) y de los sistemas que los tratan (análisis, diseño, desarrollo, implantación, explotación, integración y mantenimiento).

1.2 Acrónimos

A continuación, se incluyen los acrónimos específicos para la comprensión de los contenidos del presente documento:

- CAU: Centro de Atención al Usuario.
- DGSD: Dirección General de Salud Digital.
- GRS: Gerencia Regional de Salud de Castilla y León.
- ENS: Esquema Nacional de Seguridad.
- LOPDGDD: Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
- PSIPD: Política de Seguridad y Protección de Datos de la Gerencia Regional de Salud de Castilla y León.
- RGPD: Reglamento General de Protección de Datos.
- USB (memoria USB): Dispositivo de almacenamiento externo que permite guardar información o transferir datos entre diferentes terminales (en inglés: Universal Serie Bus).

1.3 Referencias

Los siguientes documentos son aplicables en la medida que tengan carácter contractual o hayan sido aprobados por la GRS, correspondiéndose sus versiones y fechas con las vigentes en el momento de publicación del presente; el resto se han usado simplemente a modo de soporte.

Código	Documento
[1]	Política de Seguridad de la Información y Protección de Datos de la GRS
[2]	Procedimiento de gestión de incidentes

2 CÓDIGO DE CONDUCTA Y BUENAS PRÁCTICAS PARA LOS USUARIOS DE SISTEMAS DE INFORMACIÓN DE LA GRS

1. Gestión de activos

1.1. Toda persona que preste servicios a la GRS, está obligada a proteger, de acuerdo a su calificación de seguridad, los activos puestos a su disposición para el desarrollo de sus funciones, debiendo prestar especial atención a aquellos que contengan datos personales.

1.2. Es responsabilidad de cada centro u organismo dependiente de la GRS llevar a cabo un inventario actualizado de los activos de información, teniendo en cuenta sus niveles de criticidad y sensibilidad.

1.3. Cada activo de información deberá contar con un propietario, al cual se le asignará la responsabilidad de implantar y mantener los controles necesarios para la protección de los activos.

1.4. El uso de los activos de información se deberá realizar acorde a lo establecido por la GRS en su PSIPD, en el presente código de conducta y buenas prácticas, y en el resto de normativa vigente y aplicable en la GRS.

2. Uso de equipos informáticos

2.1. Los equipos informáticos se deben utilizar exclusivamente para llevar a cabo las funciones encomendadas. No se permite el uso de equipamiento informático propiedad de la GRS para fines particulares. Dentro de esta categoría se incluyen teléfonos móviles, ordenadores portátiles y tabletas, así como cualquier otro dispositivo suministrado por la GRS.

2.2. No está permitido el uso de equipos informáticos o cualquier otro dispositivo personal para acceder a los sistemas de información de la GRS, salvo que sea autorizado por la DGSD. Asimismo, no podrán efectuarse conexiones a la red informática de la GRS desde cualquier equipo o dispositivo no facilitado por la GRS, sin previa autorización.

2.3. No se conservará en las unidades de almacenamiento local de los equipos informáticos, aquella información que contenga datos personales o cualquier otro tipo de información considerada, o no confidencial. En caso contrario, los usuarios serán responsables de la custodia y respaldo de toda la información que almacenen en los mismos.

2.4. Queda prohibido cambiar la configuración de los equipos informáticos y periféricos, salvo que se obtenga autorización expresa de la DGSD o del Servicio de Informática de su centro.

2.5. No se permite sacar los equipos fuera de las instalaciones de la GRS, salvo que estuviera previamente autorizado por las personas responsables de la GRS.

2.6. El uso de equipos informáticos propiedad de la GRS, y consecuentemente, el uso de sistemas de información, el acceso a Internet o al correo electrónico corporativo, podrá ser monitorizado y auditado en los términos que autorice la legislación vigente.

2.7. Los usuarios comunicarán al CAU cualquier incidencia de funcionamiento o deficiencia de las aplicaciones informáticas que observen, así como cualquier mejora que se estime adecuada, de acuerdo a lo establecido en la normativa interna.

3. Uso de dispositivos móviles corporativos

3.1. Los dispositivos móviles corporativos estarán registrados en la plataforma de gestión de dispositivos móviles de la GRS, con el fin de poder gestionar y proteger los datos corporativos.

3.2. Los dispositivos móviles corporativos deberán protegerse por una contraseña segura de inicio (PIN o usuario y contraseña dependiendo de cada dispositivo), la cual será requerida cada vez que el usuario encienda el dispositivo móvil.

3.3. En caso de inactividad, se deberá mantener bloqueada la pantalla del dispositivo, estando protegida por mecanismos de autenticación (como PIN, patrones, biometría).

3.4. Las contraseñas son intransferibles y el acceso al contenido del dispositivo es personal, debiéndose evitar su conexión a otros equipos ajenos, salvo autorización expresa por parte de la GRS.

3.5. Se evitará mantener en la unidad de almacenamiento local del dispositivo documentos que contengan datos personales, o cualquier otro tipo de información considerada, o no confidencial, más allá del tiempo necesario para cumplir su finalidad. Pasado dicho tiempo, los archivos deberán eliminarse de los equipos. En caso contrario, los usuarios serán responsables de la custodia y respaldo de toda la información que almacenen en los mismos, tal y como se indica en el apartado 2.3 de este código.

3.6. Se deberá cifrar cualquier información almacenada en los dispositivos móviles, todo ello con el objetivo de reducir el impacto que pudiera generar la pérdida o robo del dispositivo.

3.7. Se deberá evitar conectar los dispositivos móviles a redes públicas y redes no confiables, así como la conexión por USB a cualquier dispositivo público.

3.8. En caso de que un usuario detecte cualquier anomalía o incidente de seguridad que pudiera comprometer el buen uso y funcionamiento del dispositivo, deberá informarlo inmediatamente al CAU, para investigación y resolución del incidente.

3.9. En caso de pérdida o robo del dispositivo, el usuario deberá notificarlo a CAU o a su responsable en el menor tiempo posible desde que hubiese detectado la desaparición, para que se proceda a adoptar las medidas de seguridad que se estimen oportunas.

4. Bloqueo del puesto de trabajo

4.1. Cuando los usuarios se ausenten del puesto de trabajo o dejen desatendido el ordenador o cualquier otro dispositivo móvil que se encontrasen utilizando, deberán activar el sistema de bloqueo del que disponga el equipo (salvapantalla protegido por contraseña, bloqueo del terminal, etc.) con el fin de que se no visualicen datos en la pantalla, así como evitar que se acceda al equipo o aplicaciones por terceros no autorizados.

4.2. El puesto de trabajo se deberá bloquear de forma automática, al cabo de un tiempo de inactividad establecido por la política de seguridad, como parte de la configuración del equipo, y sin poder ser alterado por los usuarios.

5. Puesto de trabajo despejado

5.1. Los puestos de trabajo deben estar despejados, sin más material encima de la mesa que el que se requiera para la actividad que se haga en cada momento.

5.2. Los documentos en papel que contengan tanto información confidencial como datos personales deberán ser custodiados en todo momento por la persona que los estuviere utilizando, debiendo evitar el acceso a los mismos por parte de personas no autorizadas. Una vez que se haya terminado de trabajar con dichos documentos, estos deberán guardarse bajo llave, o cualquier otro mecanismo, que garantice su custodia e impida el acceso no autorizado a los mismos.

5.3. Cuando un usuario abandone su puesto de trabajo debe guardar toda la información que esté tratando, de manera que no quede desatendida (memorias USB o soportes externos de información, listas o información visible en la pantalla del ordenador, documentación sobre el propio puesto de trabajo). El material de trabajo debe guardarse en un lugar cerrado (por ejemplo, en un cajón o un armario bajo llave) o en un cuarto separado cerrado con llave, al menos fuera del horario de trabajo.

6. Uso de Internet

6.1. La utilización del acceso a Internet debe responder a fines profesionales, quedando expresamente prohibido el uso del Internet con propósitos ilegales o ajenos al ámbito profesional.

6.2. Se deberá evitar la descarga de cualquier contenido para fines ajenos a la actividad laboral, quedando expresamente prohibida la descarga y posterior almacenamiento de cualquier contenido ilegal o inadecuado, o que atente a la moral, las buenas costumbres y los valores de la entidad.

6.3. Se deberá evitar visitar sitios no oficiales, poco conocidos o de dudosa reputación, y descargar cualquier información de dichos sitios.

7. Tratamiento y uso de datos personales

7.1. Los usuarios deben acceder, exclusivamente, a la información necesaria para el desarrollo de las funciones propias de su actividad laboral, y únicamente a la que estén autorizados. Bajo ningún concepto podrán utilizar las credenciales de otra persona para acceder a equipos informáticos o a sistemas de información de la GRS.

7.2. Todas las personas que intervengan en cualquier fase del tratamiento de datos personales están sujetas al deber de secreto, de forma indefinida, incluso después de haber concluido la relación que justificaba esta intervención.

7.3. Los usuarios que necesiten bajo una justificación extraer datos personales fuera de las instalaciones de la GRS, deberán solicitar la autorización pertinente del Responsable del tratamiento o del Responsable de la seguridad de su centro.

7.4. Cualquier incidencia o anomalía que pudiera afectar a la seguridad de los datos personales deberá ser comunicada al CAU o Responsable de la seguridad de su centro, quien en cada caso deberá actuar conforme a lo indicado en el procedimiento de gestión de incidentes desarrollado por la GRS.

7.5. Con la finalidad exclusiva de lograr el cumplimiento del ENS y sobre la base de un interés legítimo y proporcionado, con plenas garantías del derecho al honor, a la intimidad personal y familiar, a la propia imagen de los usuarios, y de conformidad con lo dispuesto en la normativa sobre protección de datos personales, se registrarán las actividades llevadas a cabo mediante los sistemas de información de la GRS, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

7.6. Toda entidad dependiente de la GRS está obligada a aplicar las medidas de seguridad necesarias para garantizar la confidencialidad, integridad, disponibilidad, y resiliencia permanente de los activos y sistemas de información de la GRS. En caso de que resulte necesario la externalización de servicios, se deberán evaluar los proveedores teniendo en cuenta lo dispuesto en la normativa vigente en materia de protección de datos y seguridad de la información. Asimismo, en aquellos casos en que los proveedores puedan tener acceso a información confidencial o sensible, o a los datos personales de los cuales la GRS sea responsable, se deberán suscribir los

correspondientes acuerdos de confidencialidad y deber de secreto, así como los contratos que resulten necesarios de conformidad con la normativa vigente.

8. Seguridad y privacidad desde el diseño y por defecto

8.1. Los tratamientos de datos personales se llevarán a cabo en cumplimiento del principio de privacidad desde el diseño y por defecto. Para ello, el responsable del tratamiento identificará los requisitos normativos, organizativos, técnicos y legales y establecerá los medios y las medidas técnicas y organizativas apropiadas para garantizar la seguridad y la protección de los datos, desde las primeras etapas del ciclo de vida de los datos y de los sistemas.

8.2. Los responsables de proyectos y aplicaciones se encargarán de velar por la seguridad de los mismos, garantizando que se aplican y se revisan dichas medidas de seguridad, a fin de comprobar su idoneidad y que no comprometen la seguridad del sistema, ni el derecho a la protección de datos de las personas físicas. En todo caso, informarán de los proyectos y/o aplicaciones al Responsable de la seguridad de su centro y a la DGSD.

8.3. El personal de la GRS, así como el personal de las empresas externas, públicas y privadas deberá realizar los tratamientos de datos personales siguiendo las instrucciones establecidas por el responsable del tratamiento y utilizando exclusivamente los medios dispuestos para ello.

9. Protección de datos personales

9.1. Los usuarios con acceso a datos personales y/o sistemas de información que tratan datos personales están obligados a cumplir las medidas de seguridad establecidas y los requisitos y las condiciones aplicables de acuerdo con las normas y los procedimientos vigentes en la GRS.

9.2. Los usuarios deben conocer los principios básicos del RGPD y la LOPDGDD relativos al tratamiento de datos personales requerido para desempeñar sus funciones. A continuación, se detallan algunas consideraciones esenciales sobre dichos principios:

i. Todos los usuarios que tengan acceso a datos personales deben conocer la finalidad de usarlos y sus obligaciones particulares relativas al tratamiento requerido en el desempeño de su actividad profesional.

ii. Los datos personales han de ser exactos y actualizados; por ello deben adoptarse todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos respecto a los fines para los que se tratan.

iii. Los usuarios que tengan acceso a datos personales deben extremar las precauciones para evitar la difusión o el acceso no autorizado y no tratarlos sin la autorización previa del responsable de tratamiento. Las cesiones de datos deben contar con habilitación legal y conforme a las medidas de seguridad aplicables, aunque es preferible siempre que sea posible comunicar solamente datos seudonimizados o anónimos.

iv. Debe accederse a la información que contenga datos personales solamente por medio de los procedimientos habilitados a tal efecto por la GRS.

v. Cualquier requerimiento nuevo para el tratamiento de datos personales que sea identificado —fuera de la actividad prevista— debe ser analizado y autorizado previamente por la persona que ejerce el cargo de Delegado de Protección de Datos de la GRS.

vi. Todos los usuarios deben colaborar para satisfacer el ejercicio de cualquiera de los derechos de los interesados (acceso, rectificación, supresión, oposición, portabilidad, limitación del tratamiento y no ser objeto de elaboración de

perfiles), atendiéndoles e informándoles sobre el procedimiento que deben seguir.

vii. Cualquier iniciativa, proyecto o desarrollo que vaya a iniciarse dentro de la GRS debe pasar por una fase de análisis de la privacidad desde el diseño y por defecto.

9.3. Todo tratamiento que deba hacerse fuera de los sistemas de información de la GRS tiene que ser autorizado previamente por el Responsable del tratamiento y ha de cumplir las medidas necesarias para proteger la información.

9.4. Cuando se envíen por primera vez datos personales en formato electrónico o impresos en papel, se debe validar el método de envío a fin de garantizar que se cumplen las medidas de seguridad requeridas por el tratamiento.

9.5. Para tratar documentación que contenga datos personales es necesario respetar las siguientes directrices:

i. A no ser que sea estrictamente necesario, hay que evitar imprimir en papel documentación que contenga datos personales.

ii. No dejar documentos impresos con datos personales o confidenciales en la bandeja de salida de impresoras ni en los faxes. De la misma manera, evitar hacer fotocopias de dichos documentos, y si se hacen, controlar el uso que se les da y destruirlas oportunamente.

iii. Los documentos deben guardarse en cajones o en armarios bajo llave en los periodos de ausencia del puesto de trabajo.

9.6. Los documentos impresos u otros medios físicos que contengan datos personales deben eliminarse de manera segura con máquinas destructoras de papel o mecanismos similares. Cada usuario debe revisar periódicamente los documentos que estén bajo su custodia y destruir los que sean obsoletos. En caso de ser necesario generar archivos temporales, que contengan datos personales, deben tomarse las siguientes medidas:

i. Ha de garantizarse que el tratamiento cumple las finalidades autorizadas.

ii. Han de cumplirse todas las medidas de seguridad establecidas de acuerdo con el nivel de riesgo identificado.

iii. Han de alojarse los datos temporales en las unidades ofimáticas (carpetas) asignadas a los usuarios por las unidades responsables en materia de tecnología de la información a fin de garantizar los controles técnicos preestablecidos, y evitar alojarlos en un ordenador personal, siempre que sea posible.

iv. Han de eliminarse o destruirse de manera segura los archivos cuando dejen de ser necesarios para la finalidad para la que hayan sido creados.

9.7. Cualquier incidencia o anomalía que pueda afectar a la seguridad de los datos personales debe comunicarse al CAU o al Servicio de Informática de su centro, de acuerdo con el procedimiento de gestión de incidentes de seguridad vigente.

10. Incidentes de seguridad

10.1. El personal de la GRS, así como el personal de las empresas externas, públicas y privadas, deberán conocer el procedimiento de gestión de incidentes de seguridad vigente en la GRS.

10.2. En caso de detectar algún incidente, todo el personal está obligado a reportarlo mediante la herramienta de gestión de peticiones internas o comunicarlo al CAU, o al contacto designado (en caso de terceros), a la mayor brevedad posible. Se deberá reportar el detalle de los hechos acontecidos y de las medidas adoptadas, a fin de que se tomen las decisiones oportunas por las personas responsables de la GRS.

10.3. Los incidentes de seguridad se gestionarán por el equipo de respuesta de incidentes, nunca por parte de la persona que los detecte. Dicho equipo, en cumplimiento de la normativa interna, evaluará el incidente y lo comunicará a los organismos

correspondientes, en caso de que el incidente cumpla con los supuestos de notificación exigidos por la normativa vigente en materia de seguridad de la información y protección de datos personales.

10.4. El Responsable de la seguridad de la GRS y el Responsable de la seguridad delegado en cada centro, en su caso, podrán, de oficio, conforme a lo dispuesto en la PSIPD, y cuando razones de urgencia así lo justifiquen, proceder, de forma inmediata y directa, a realizar las acciones necesarias sobre el hardware o software de cualquier persona usuaria (incluyendo su retirada), reportando esta acción, y su justificación, en cuanto sea posible, a quien corresponda.

11. Uso de contraseñas

11.1. Las cuentas de los usuarios y sus credenciales de acceso (usuario y contraseñas), son personales e intransferibles. En consecuencia, no se deberán facilitar a otras personas

11.2. Se deberán utilizar contraseñas seguras, siguiendo las normas de complejidad y robustez frente a ataques de adivinación, según lo dispuesto en política de contraseñas seguras de la GRS.

11.3. Los usuarios deben ser cuidadosos y diligentes en la custodia y manejo de las contraseñas y mantenerlas en secreto. En caso de pérdida de la contraseña o que la misma resulte comprometida, el usuario deberá informar al CAU y proceder con el cambio inmediato de la misma.

11.4. Los usuarios son los únicos autorizados para el uso de las cuentas que le hubieren sido asignadas, y son responsables de las acciones que se realicen con su identidad en los sistemas de información.

11.5. Las contraseñas de acceso a los servicios corporativos de la GRS no se deberán utilizar para otros servicios u otras cuentas no corporativas.

12. Uso de certificados digitales

12.1. Los usuarios deberán hacerse responsables de salvaguardar sus claves privadas, y cualquier elemento que pueda ser necesario para acceder a las mismas (tarjeta o dispositivo criptográfico, archivo informático, programa software, etc.) o código (PIN, contraseña, etc.), aplicando las pautas descritas en el apartado 8 del presente código.

12.2. Los usuarios comunicarán al CAU cualquier compromiso de su clave privada, o de los elementos y códigos utilizados para su acceso, a la mayor brevedad.

12.3. Los usuarios deberán respetar las garantías y requisitos suscritos por la GRS y por la correspondiente Entidad Prestadora de Servicios de Certificación, así como la correspondiente Declaración de Prácticas de Certificación de la Autoridad de Certificación relevante, con respecto a la provisión de servicios técnicos, administrativos y de seguridad necesarios para garantizar la validez de las transmisiones electrónicas emitidas y recibidas.

13. Uso del correo electrónico

13.1. El servicio de correo electrónico de la GRS es de uso obligatorio y únicamente se utilizará por aquellos usuarios a los que se les haya dotado de cuenta de correo, para uso exclusivo en el desempeño de sus funciones.

13.2. La cuenta de correo electrónico es intransferible, no permitiéndose la cesión de la misma.

13.3. Con carácter general, está prohibido el envío de datos de salud o de cualquier otra información sensible mediante correo electrónico. En caso de ser necesario tal envío, los datos deberán ser cifrados y debidamente autorizados por el Responsable del tratamiento, tal y como se indica en el apartado 16.2 del presente código de conducta y buenas prácticas.
13.4. Para evitar el correo masivo no solicitado (spam), como regla general, solo se debe proporcionar la dirección de correo electrónico a personas y entidades conocidas, para uso exclusivamente profesional y no debiéndose utilizar la dirección de correo electrónico en foros o páginas web no institucionales.
13.5. Cuando se reciban correos electrónicos desconocidos o no solicitados, no se deben contestar, ya que al hacerlo se reconfirma la dirección.
13.6. En el caso de recibir correos electrónicos cuyo remitente, o contenido, o ambos, sea dudoso, se evitará abrir el correo, siendo necesario contactar con el CAU para que se analice su posible legitimidad.
13.7. Cuando resulte necesario realizar un envío masivo de correos electrónicos, se deberán añadir las direcciones de correo en copia oculta (CCO).
13.8. Queda prohibido el uso de cuentas de correo electrónico externas para el envío y recepción de información corporativa, permitiendo el uso únicamente de aquellas cuentas de correo habilitadas por la GRS para tal fin.

14. Software. Protección contra el código dañino

14.1. Las aplicaciones informáticas se mantendrán actualizadas y con los últimos parches de seguridad aplicados por la DGSD o por el Servicio de Informática de su centro.
14.2. Se prohíbe la instalación de software o programas no corporativos en los equipos informáticos de la GRS. Si fuera necesaria su instalación, deberá solicitarse a la DGSD o al Servicio de Informática de su centro. De igual modo, no se podrán realizar copias del software instalado en dichos equipos.
14.3. Los servicios de soporte correspondientes, así como la DGSD o el Servicio de Informática, quedan facultados para que de forma directa o remota actúen sobre este software no permitido.
14.4. Los usuarios no podrán modificar el software instalado a nivel corporativo, que en ningún caso deberá ser desinstalado o desactivado.
14.5. Los puestos de usuario deben disponer de mecanismos adecuados para el control de software malicioso (virus, gusanos, etc.), que han de permanecer activados y actualizados. Ante la sospecha de una infección por software malicioso, se deberá comunicar la incidencia al CAU, sin dilaciones.

15. Uso de redes sociales

15.1. Con carácter previo a darse de alta con el perfil de profesional o perfil corporativo en una red social, se deberá obtener el consentimiento de la organización o del centro adscrito a la GRS.
15.2. El usuario autorizado a darse de alta con perfil corporativo deberá asegurarse de leer las Políticas de uso y de privacidad de los diferentes servicios, y no deberá basarse en la configuración por defecto que proporcione la plataforma.
15.3. El contenido a publicar por el usuario deberá ser previamente autorizado por la organización o centro. Bajo ninguna circunstancia se podrá difundir información confidencial o datos sensibles de la GRS. De igual modo, se deberá evitar publicar comentarios despectivos ni ofensivos.
15.4. En caso de que la publicación incluya datos personales de terceros o información sobre otro organismo, se deberá obtener previamente su consentimiento para la difusión.

15.5. El usuario de una red social con un perfil corporativo de la GRS deberá evitar acceder a enlaces de dudosa procedencia, o a sitios que puedan poner en riesgo los sistemas de información de la entidad. De igual modo, se deberá evitar descargar ficheros de fuentes no confiables, tal y como se indica en el punto 4.2 del presente código de conducta y buenas prácticas.

16. Transferencia de información

16.1. La entrada y salida de cualquier información realizada en el entorno corporativo de la GRS a través de las redes de comunicación, y de manera especial, la información confidencial o que contenga datos personales y/o sensibles, deberá realizarse haciendo uso de los servicios corporativos aprobados y que la GRS pone a disposición de sus usuarios (carpetas compartidas, correo electrónico, servicios de gestión documental y colaborativos, etc.). Queda prohibido el uso de cualquier otra herramienta de transferencia de información que no haya sido previamente aprobada por la GRS.

16.2. En caso de que la información que se pretenda transferir contenga información confidencial, de alto contenido sensible o incluya datos personales, se deberá cifrar antes de su transmisión.

16.3. Para el uso, determinación y aplicación de controles criptográficos en los soportes de información de la GRS, se deberá tener en cuenta aquellos mecanismos acreditados por el Centro Criptológico Nacional, y, asimismo, certificados por normas europeas o estándares internacionales.

16.4. Se eliminarán los metadatos y marcas de los documentos antes de que sean compartidos o publicados, salvo que esta información deba estar presente en el documento a difundir.

17. Destrucción de la información

17.1. Cuando un soporte informático (disco duro, USB, CD, etc.) o documento (en formato electrónico o papel), contenga datos personales u otro tipo de información, incluso pública, y vaya a ser desechado, se deberán adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada o impresa. En caso de que la información que se pretenda destruir esté en soporte de papel, se deberá hacer uso de las destructoras de papel o de los contenedores de depósito y destrucción segura y certificada de documentación de los que disponga en la GRS.

17.2. Cada área o centro deberá contar con un procedimiento para la destrucción de soportes y de documentación, teniendo en cuenta lo establecido en este código de conducta y buenas prácticas, así como lo dispuesto en la PSIPD y demás normativa que resulte de aplicación.

18. Sistemas de almacenamiento de información en la nube

18.1. No está permitido transmitir o alojar datos personales o información propia de la GRS en servidores externos o soluciones de almacenamiento en la nube distintas a las soluciones corporativas, salvo que se disponga de autorización previa por parte de la DGSD.

18.2. Con carácter previo al uso de recursos en la nube, la DGSD establecerá las características del servicio prestado y las responsabilidades de las partes, detallando lo que se considera calidad mínima del servicio prestado y las consecuencias de incumplirlo.

18.3. Se deberá comprobar que no haya impedimentos legales y verificar la suscripción de un contrato expreso entre la GRS y la empresa responsable de la prestación del servicio en la nube, incluyendo los acuerdos de nivel de servicio que sean procedentes, el correspondiente acuerdo de confidencialidad, y siempre habiendo analizado previamente los riesgos asociados.

19. Uso de herramientas de mensajería instantánea y sistemas de videoconferencia

19.1. La GRS dotará al personal de herramientas de comunicación, mensajería instantánea y sistemas de videoconferencias que cumplan los requerimientos legales vigentes.

19.2. En ningún caso se deben utilizar servicios de mensajería instantánea o sistemas de videoconferencia no autorizados por la GRS.

20. Teletrabajo

20.1. En la modalidad de teletrabajo, los usuarios deben aplicar todas las medidas aconsejadas descritas en los puntos precedentes y las que se describen a continuación.

20.2. Como norma general, se deben usar los equipos de trabajo facilitados por la GRS que están equipados con las medidas de seguridad corporativas. Si se recibe autorización para usar un equipo personal, se deberán seguir las pautas y recomendaciones de seguridad siguientes a fin de proteger adecuadamente la información y las comunicaciones:

i. Se han de crear contraseñas robustas y usar el doble factor de autenticación, tal como se le indicará por la DGSD.
ii. Se deben mantener actualizados el sistema operativo y los programas instalados, tanto los de uso corporativo como los de nivel de usuario. Si se descargan otros programas, debe asegurarse que provienen de fuentes oficiales y que están autorizados.
iii. Se ha de disponer de un sistema antivirus actualizado periódicamente.
iv. Se deben cifrar los soportes de información a fin de proteger su contenido de posibles accesos malintencionados y, de esta manera, garantizar su confidencialidad e integridad.
v. Se han de realizar copias de seguridad periódicamente.
vi. En ningún caso los usuarios pueden trabajar con un equipo público que no sea el propio (p. ej., de un cibercafé, un hotel, un aeropuerto…).
vii. Siempre que sea posible se debe usar la red doméstica y evitar las redes Wifi-públicas. Si no es posible usar la red doméstica o, como alternativa, cualquier otra red que se considere segura, se recomienda que se use la red de datos móviles propia.
viii. Se ha de acceder a la red interna y a los sistemas de información de la GRS usando exclusivamente los mecanismos corporativos habilitados, como las redes privadas virtuales o los servicios de acceso remoto seguro.
ix. Para participar en reuniones virtuales o hacer videollamadas, se deberán utilizar exclusivamente las herramientas corporativas habilitadas para tal efecto.

20.3. La GRS podrá en cualquier momento limitar el acceso a sus redes y servicios publicados en Internet a los equipos de los usuarios que no cumplan los requisitos mínimos de seguridad establecidos.

21. Finalización de la vinculación o relación con la GRS

21.1. Cuando un usuario finaliza su relación o vinculación con la GRS, dejará de tener acceso a los sistemas de información de la GRS y a los datos que estos contienen. Asimismo, deberá devolver cualquier soporte que posea y que contenga datos a los que haya tenido acceso en el marco de su vinculación o relación con la GRS.

21.2. También deberá ceder el control y/o entregar cualquier archivo o documento relativo a su prestación profesional; en caso de que haya creado archivos o documentos de carácter no profesional, deberá eliminarlos.

21.3. Por su parte, la GRS procederá a desactivar las credenciales de acceso a la cuenta de correo corporativa y a los sistemas de información a los que tuviera acceso el usuario.

22. Cumplimiento del código de conducta y buenas prácticas

22.1. Todos los usuarios de la GRS deben obligatoriamente cumplir el presente código de conducta y buenas prácticas.

22.2. Adicionalmente, los requisitos y las previsiones descritas en el código de conducta y buenas prácticas se complementan con el resto de la normativa vigente y con cualquier disposición legal de ámbito estatal o comunitario aplicable.

22.3. El incumplimiento de cualquiera de las pautas de comportamiento contenidas en el presente código podrá derivar en la correspondiente responsabilidad disciplinaria, si a ello hubiere lugar, en aplicación de las normas reguladoras del régimen jurídico disciplinario.

22.4. El uso de los recursos informáticos que la GRS pone a disposición de los usuarios implica el conocimiento y la aceptación plena de las normas de uso, de las condiciones y de las advertencias legales que se especifican en el presente código de conducta y buenas prácticas.

22.5. El Comité de Seguridad de la Información ha de velar por que se cumpla el presente código de conducta y buenas prácticas.