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 LEON.

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

Uso de equipos informáticos

- Los equipos informáticos (móviles, ordenadores, portátiles y tabletas) se deben utilizar exclusivamente para llevar a cabo las funciones encomendadas.
- 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.
- No se conservará en las unidades de almacenamiento local de los equipos, 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.
- El uso de equipos informáticos propiedad de la GRS y 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.
- 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.

Bloqueo del puesto de trabajo

- Cuando los usuarios se ausenten del puesto de trabajo deberán activar el sistema de bloqueo del que disponga el equipo (salvapantalla protegido por contraseña, bloqueo del terminal, etc.).
- El puesto de trabajo se deberá bloquear de forma automática, al cabo de un tiempo de inactividad.

Puesto de trabajo despejado

- 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.
- 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.
- Si se abandona el puesto de trabajo, se debe guardar toda la información que esté tratando.

Uso de Internet

- La utilización del acceso a Internet debe responder a fines profesionales.
- Se deberá evitar la descarga de cualquier contenido para fines ajenos a la actividad laboral.
- Se deberá evitar visitar sitios no oficiales, poco conocidos o de dudosa reputación, y descargar cualquier información.

Tratamiento y uso de datos personales

- Los usuarios deben acceder, usando sus credenciales, exclusivamente, a la información necesaria para el desarrollo de las funciones propias de su actividad laboral, y únicamente a la que estén autorizados.
- 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.
- Los usuarios que necesiten, bajo 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.

- 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.

Protección de datos personales

- Los usuarios con acceso a 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.
- Los usuarios deben conocer los principios básicos del RGPD y la LOPDGDD relativos al tratamiento de datos personales requerido para desempeñar sus funciones. Consideraciones esenciales sobre dichos principios:
  - 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.
  - Los datos personales han de ser exactos y actualizados.
  - 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.
  - Debe accederse a la información que contenga datos personales solamente por medio de los procedimientos habilitados a tal efecto por la GRS.
  - Cualquier requerimiento nuevo para el tratamiento de datos personales que sea identificado —fuera de la actividad prevista— debe ser analizado y autorizado previamente.
  - 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.
- Todo tratamiento 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.
- Cuando se envíen 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.
- Para tratar documentación que contenga datos personales es necesario respetar las siguientes directrices:
  - A no ser que sea estrictamente necesario, evitar imprimir en documentación que contenga datos personales.
  - No dejar documentos impresos con datos personales o confidenciales en las bandejas de salida.
  - Los documentos deben guardarse bajo llave en los periodos de ausencia del puesto de trabajo.
- Los documentos impresos u otros medios físicos que contengan datos personales deben eliminarse de manera segura con máquinas destructoras de papel o mecanismos similares. En caso de ser necesario generar archivos temporales, que contengan datos personales, deben tomarse las siguientes medidas:
  - Ha de garantizarse que el tratamiento cumple las finalidades autorizadas.
  - Han de cumplirse todas las medidas de seguridad establecidas de acuerdo con el nivel de riesgo identificado.
  - Han de alojarse los datos temporales en las unidades ofimáticas (carpetas) asignadas a los usuarios.
  - Han de eliminarse o destruirse de manera segura los archivos cuando dejen de ser necesarios para la finalidad para la que hayan sido creados.
- 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.

Incidentes de seguridad

- 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.
- 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).
- Los incidentes de seguridad se gestionarán por el equipo de respuesta de incidentes.
- 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, proce-

der, de forma inmediata y directa, a realizar las acciones necesarias sobre el hardware o software de cualquier persona usuaria (incluyendo su retirada).

Uso de contraseñas

- Las cuentas de los usuarios y sus credenciales de acceso (usuario y contraseñas), son personales e intransferibles.
- Se deberán utilizar contraseñas seguras, siguiendo las normas de complejidad y robustez.
- 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.
- Las contraseñas de acceso a los servicios corporativos de la GRS no se deberán utilizar para otros servicios u otras cuentas no corporativas.

Uso de certificados digitales

- *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.*
- *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.*
- *Los usuarios deberán respetar las garantías y requisitos suscritos por la GRS y por la correspondiente Entidad Prestadora de Servicios de Certificación.*

Uso de correo electrónico

- El servicio de correo electrónico de la GRS es de uso obligatorio y para uso exclusivo para sus funciones.
- 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.
- 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, no se debé utilizar la dirección de correo electrónico en foros o páginas web no institucionales.
- Cuando se reciban correos electrónicos desconocidos, no solicitados o dudosos, no se deben contestar, ya que al hacerlo se reconfirma la dirección, siendo necesario contactar con el CAU para que se analice su posible legitimidad.
- 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.

Software. Protección contra el código dañino

- 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.
- Los usuarios no podrán modificar el software instalado a nivel corporativo, que en ningún caso deberá ser desinstalado o desactivado.
- Los puestos de usuario deben disponer de mecanismos adecuados para el control de software malicioso, permanecer activados y actualizados, y comunicar cualquier incidencia al CAU, sin dilaciones.

Uso de redes sociales

- 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, y deberá asegurarse de leer las Políticas de uso y de privacidad de los diferentes servicios.
- El contenido a publicar por el usuario deberá ser previamente autorizado por la organización o centro.
- 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.

Transferencia de información

- Queda prohibido el uso de cualquier herramienta de transferencia de información que no haya sido previamente aprobada por la GRS (carpetas compartidas, correo electrónico, servicios de gestión documental, etc).
- 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.
- 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.

Sistemas de almacenamiento de información en la nube

- 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.

Uso de herramientas de mensajería instantánea y sistemas de videoconferencia

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

Teletrabajo

- 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:
  - Se han de crear contraseñas robustas y usar el doble factor de autenticación.
  - Se deben mantener actualizados el sistema operativo y los programas instalados, tanto los de uso corporativo como los de nivel de usuario.
  - Se ha de disponer de un sistema antivirus actualizado periódicamente.
  - Se deben cifrar los soportes de información a fin de proteger su contenido de posibles accesos malintencionados.
  - No se puede trabajar con un equipo público que no sea el propio (p. ej., de un cibercafé, un hotel…).
  - Siempre que sea posible se debe usar la red doméstica y evitar las redes Wifi-públicas.
  - 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.
- 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.

Finalización de la vinculación o relación la GRS

- 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.
- 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.
- 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.