INFORMACIÓN A TODOS LOS INVESTIGADORES DEL IISGM

NOTA SOBRE BUENAS PRÁCTICAS PARA USUARIOS DE SISTEMAS DE INFORMACIÓN DE LA CONSEJERÍA DE SANIDAD

Enero 2018

Para mantener en óptimas condiciones los sistemas de información que usamos en el entorno de la Comunidad de Madrid y evitar problemas que pueden tener graves consecuencias, les recordamos que existe la orden *ORDEN 491/2013, de 27 de junio, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica y de los sistemas de información de la Consejería de Sanidad de la Comunidad de Madrid,* y que esta tiene un anexo de **Buenas Prácticas Para Usuarios De Sistemas De Información De La Consejería De Sanidad** que reproducimos a continuación y que rogamos tengan a bien de leer y tener en cuenta.

Muchas gracias

Fundación para la Investigación Biomédica del Hospital Gregorio Marañón

FUNDACIÓN INVESTIGACIÓN BIOMÉDICA · HOSPITAL GREGORIO MARAÑÓN · ADMINISTRACIÓN

PABELLON DE GOBIERNO
Doctor Esquerdo, 46
28007 Madrid
Tel. 914 265115
Fax 914 008156

ANEXO

DECÁLOGO DE BUENAS PRÁCTICAS PARA USUARIOS DE SISTEMAS DE INFORMACIÓN DE LA CONSEJERÍA DE SANIDAD

1. Uso de los equipos informáticos.

1.1. Los equipos informáticos no deben ser utilizados para fines particulares.

1.2. No deben almacenarse en la memoria de los ordenadores documentos que contengan datos de carácter personal. En caso contrario, los usuarios serán responsables de la custodia y respaldo de toda la información que almacenen en los mismos.

1.3. No se podrán modificar los equipos informáticos y periféricos, así como su conexión a otros equipos ajenos a la CSCM, salvo que se obtenga autorización expresa de quien corresponda.

1.4. No se deberán sacar equipos fuera de las instalaciones, excepto que estuviera previamente autorizado por el responsable de seguridad designado conforme la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

1.5. Los usuarios comunicarán al responsable informático del centro, y/o al centro de soporte a usuarios, cualquier incidencia de funcionamiento o deficiencia de las aplicaciones informáticas que hubieran podido observar, así como cualquier mejora que se estime adecuada.

1.6. Cuando una incidencia y/o deficiencia pudiera causar un elevado impacto en el funcionamiento del servicio sanitario, los usuarios, de acuerdo siempre con el centro de soporte a usuarios, podrán adoptar las medidas de urgencia que se estimen oportunas. El detalle de los hechos acontecidos y de las medidas adoptadas se deberá poner en conocimiento de quien corresponda a fin de que éste tome las decisiones oportunas.

2. Internet.

2.1. La utilización del acceso a Internet debe responder a fines profesionales.

2.2. El uso de los sistemas de información tales como el acceso a Internet o el correo electrónico corporativo, podrá ser auditado en los términos que autorice la legislación vigente.

3. Tratamiento y uso de datos de carácter personal.

3.1. Los usuarios deben acceder, exclusivamente, a la información necesaria para el desarrollo de las funciones propias de su actividad y únicamente a la que esté autorizado.

3.2. En el acceso a ésta información los usuarios están obligados a cumplir todas las medidas de seguridad establecidas por la normativa en protección de datos, y demás requisitos aplicables conforme a las normas y procedimientos establecidos en la CSCM.

3.3. Todas las personas que intervengan en cualquier fase del tratamiento de datos de carácter personal están obligadas al secreto profesional respecto de los mismos.

3.4. Cuando un soporte informático (disco duro, USB, CD...), o documento, en formato electrónico o papel, contenga datos personales, y vaya a ser desechado, se deberán adoptar las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada o impresa en los mismos.

3.5. El personal que necesite extraer de la CSCM datos de carácter personal deberá solicitar la autorización pertinente del Responsable de Seguridad, conforme a la Ley

PABELLON DE GOBIERNO
Doctor Esquerdo 46
28007 Madrid
Tel 914 265115
Fa 914 008156

Orgánica 15/1999, de 13 de diciembre, y aplicar las debidas medidas de seguridad para proteger esa información. Asimismo, el Responsable de Seguridad deberá llevar un registro actualizado de la salida de esta información.

3.6. Cualquier incidencia o anomalía que pudiera afectar a la seguridad de los datos personales deberá ser comunicada al responsable de seguridad del centro y al Área de Seguridad.

3.7. Los accesos a los sistemas de información podrán ser monitorizados y registrados para auditar el uso de los mismos, de conformidad con lo estipulado en el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Incidentes de seguridad de la información.

4.1. Cuando ocurra un incidente que afecte a la seguridad de la información, el usuario deberá reportar el detalle de los hechos acontecidos y de las medidas adoptadas a su superior jerárquico y/o al Área de Seguridad, a fin de que se tomen las decisiones oportunas.

4.2. Asimismo, el Responsable de Seguridad podrá, de oficio, conforme el artículo 6.3.c de la Política de Seguridad de la Información, 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 usuario (incluyendo la retirada de los mismos), reportando esta acción, en cuanto sea posible, a quien corresponda.

5. Uso de contraseñas.

5.1. Tanto las cuentas de usuario como las contraseñas son personales. En consecuencia, no se deberán facilitar a otros usuarios, salvo que se reciba autorización expresa del Responsable de Seguridad y/o responsable de informática, conforme la Ley Orgánica 15/1999, de 13 de diciembre.

5.2. Los usuarios deben ser cuidadosos y diligentes en la custodia y cuidado de las contraseñas y deben mantenerlas en secreto, debiendo informar en caso de pérdida o compromiso de la misma.

5.3. Los usuarios son los únicos autorizados para el uso de la cuenta, y deben ser conscientes de que son responsables de las acciones que se realicen con su identidad en los sistemas de información.

6. Uso de certificados digitales.

6.1. Los usuarios deberán hacerse responsables de salvaguardar sus claves privadas, aplicando las pautas descritas en el apartado 5.2 del presente Decálogo, y al de cualquier elemento (tarjeta o dispositivo criptográfico, archivo informático, programa "software", etcétera) y/o código (PIN, contraseña, etcétera) que puedan ser necesarios para acceder a las mismas.

6.2. Los usuarios comunicarán a la oficina de registro del centro correspondiente, o a la Entidad Prestadora de Servicios de Certificación y/o registro, cualquier compromiso de su clave privada, o de los elementos y/o códigos utilizados para su acceso, a la mayor brevedad.

6.3. Los usuarios deberán respetar las garantías y requisitos suscritos por la CSCM 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

FUNDACIÓN INVESTIGACIÓN BIOMÉDICA · HOSPITAL GREGORIO MARAÑÓN · ADMINISTRACIÓN

PABELLON DE GOBIERNO
Doctor Esquerdo, 46
28007 Madrid
Tel. 914 265115
Fax. 914 008156

necesarios para garantizar la validez de las transmisiones electrónicas emitidas y recibidas.

7. Correo de la CSCM.

7.1. El servicio de correo electrónico de la CSCM es de uso obligatorio y únicamente se utilizará por aquellos usuarios a los que se les haya dotado de cuenta de correo para uso profesional, debiendo observarse el deber de diligencia en la utilización del mismo.

7.2. Deberá minimizarse el uso del correo de la CSCM con fines distintos a los laborales.

7.3. Con carácter general, está prohibido el envío de datos de salud fuera de la red de la CSCM mediante correo electrónico. En caso de ser necesario tal envío, los datos deberán ser cifrados. En cualquier caso, debe observarse lo descrito en el apartado 2.7 del presente Decálogo.

7.4. Para evitar el correo masivo no solicitado, también denominado "spam", como regla general, solo se debe dar nuestra dirección de correo electrónico a personas y/o entidades conocidas. No se debe introducir la dirección de correo electrónico en foros o páginas Web no institucionales. Cuando se reciban correos electrónicos desconocidos o no solicitados no se deben contestar, ya que al hacerlo se reconfirma la dirección.

7.5. En el caso de recibir correos electrónicos cuyo remitente y/o contenido sea dudoso, deberá ponerse en contacto con el centro de soporte de usuarios para que se analice su posible malignidad, conforme el apartado 8 del presente Decálogo.

8. Virus informáticos y otro tipo de "malware".

8.1. Todos los puestos de la CSCM deben disponer de mecanismos adecuados para el control de "software" malicioso (virus, gusanos, etcétera), y han de permanecer activados. No está permitida la desactivación de dichos mecanismos.

8.2. Ante la sospecha de una infección por virus, gusanos, etcétera, se deberá comunicar la incidencia al centro de soporte de usuarios.

9. "Software".

9.1. Debido a la naturaleza dinámica y cambiante de los requisitos que han de satisfacer, las aplicaciones informáticas han de mantenerse siempre actualizadas, para lo cual resulta imprescindible la colaboración de todos y cada uno de los usuarios.

9.2. Para preservar el buen funcionamiento de los sistemas de información se prohíbe la instalación de "software" o programas no corporativos en los ordenadores. Si fuera necesaria su instalación, deberá solicitarse al responsable correspondiente para que lo gestione. Igualmente, no se podrán realizar copias del "software" instalado en los ordenadores.

9.3. Los servicios de soporte correspondientes, así como el Área de Seguridad, quedan facultados para que de forma directa o remota actúen sobre este "software" no permitido.

9.4. Los usuarios no podrán modificar el "software" instalado a nivel corporativo, que en ningún caso deberá ser desactivado.

10. Mesas limpias y bloqueo del ordenador.

10.1. Cuando los usuarios se ausenten del puesto de trabajo o dejen desatendido el ordenador deberán activar el sistema de bloqueo del que disponga su equipo (salvapantalla protegida por contraseña, bloqueo del terminal, etcétera) 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.

FUNDACIÓN INVESTIGACIÓN BIOMÉDICA · HOSPITAL GREGORIO MARAÑÓN · ADMINISTRACIÓN

PABELLON DE GOBIERNO
Doctor Esquerdo 46
28007 Madrid
Tel 914 265115
Fax 914 008156

10.2. Del mismo modo todos los documentos en papel que contengan datos de carácter personal deberán ser custodiados en todo momento, mientras estén siendo usados, por la persona a cargo, evitando el acceso por personas no autorizadas. Una vez que se haya terminado de trabajar con dichos documentos estos deberán guardarse bajo llave o utilizando cualquier otro mecanismo que garantice su custodia e impida el acceso a los mismos.

El incumplimiento de cualquiera de las pautas de comportamiento contenidas en el presente Decálogo de buenas prácticas podrá dar lugar a la correspondiente responsabilidad disciplinaria, si a ello hubiere lugar, en aplicación de las normas reguladoras del régimen jurídico disciplinario propio del usuario.

FUNDACIÓN INVESTIGACIÓN BIOMÉDICA · HOSPITAL GREGORIO MARAÑÓN · ADMINISTRACIÓN

PABELLON DE GOBIERNO
Doctor Esquerdo, 46
28007 Madrid
Tel 914 265115
Fax 914 008156