Hospital Guadarrama

SaludMadrid

MADRID excelente EMPRESA CERTIFICADA

Fecha: 27/11/2023

Edición: 08

POLÍTICA DE SEGURIDAD

PARA EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

Autores:

Comité de Seguridad de la Información y Protección de Datos Personales

Pasión por cuidarte

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Raquel Beltrán García Concepción Rey Benayas Juan Antonio Sánchez García	Comité de Seguridad de la Información y Protección de Datos Personales	Directora Gerente  Rosa Salazar de la Guerra
Fecha: 24/05/2011	Fecha: 06/11/2023	Fecha: 27/11/2023

CONTROL DE REVISIONES DEL DOCUMENTO		
Edición	**Fecha**	**Descripción de la modificación**
08	27/11/2023	Adaptación del documento a un lenguaje inclusivo, según el Plan de Igualdad.
07	28/10/2022	Adaptación del documento al Esquema Nacional de Seguridad 2022, mayo 2022. Pasa a llamarse Política de Seguridad.
06	28/01/2021	Adaptación a la LOPDGDD 3/2018, de 5 de diciembre.
05	Septiembre 2018	Adaptación al RGDP 2016/679de 27 de abril de 2016, en vigor desde abril del 2018.
04	Diciembre 2017	Revisión del Documento de Seguridad, nuevos miembros, revisión e inclusión de documentos y procedimientos.
03	Abril 2016	Revisión Diagnóstico de Seguridad.
02	Diciembre 2014	Revisión del documento.
01	Diciembre 2013	Actualización de documentos.
00	24/05/2011	Versión inicial.

APROBACIÓN OFICIAL DE LA POLÍTICA DE SEGURIDAD

El **HOSPITAL GUADARRAMA** aprueba, con fecha 27 de noviembre de 2023, la presente Política de Seguridad.

Con motivo de la entrada en vigor del nuevo **Esquema Nacional de Seguridad 311/2022, de 3 de mayo del 2022,** se procedió a la modificación y adaptación del Documento de seguridad y sus procedimientos de aplicación, así como a su difusión al personal del Hospital, cambiando también el nombre del documento a Política de Seguridad.

El **HOSPITAL GUADARRAMA** ha adoptado las medidas necesarias para que todos el personal del Centro esté familiarizado con el desarrollo legislativo en España del REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 **(RGPD)**, la Ley Orgánica 3/2018, de 5 de diciembre de 2020, de protección de datos personales y garantía de los derechos digitales **(LOPDGDD)** y el Esquema Nacional de Seguridad 311/2022, de 3 de mayo **(ENS 2022),** cuyas exigencias principales se desarrollan en esta política de obligado cumplimiento para todo el Centro.

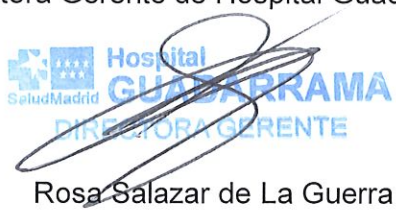
Todos los datos personales que se manejen en el Hospital, aunque sea su almacenamiento, así como todo el personal con acceso a los mismos, deberán atender y cumplir las prescripciones y medidas de seguridad contenidas en la presente Política de Seguridad.

El **HOSPITAL DE GUADARRAMA** ha establecido las funciones y responsabilidades necesarias para cumplir y hacer cumplir en todo momento la citada Legislación, haciendo especial énfasis en los procedimientos y medidas de seguridad a adoptar por el personal que tiene acceso a datos de carácter personal.

Esta política se mantendrá actualizada y será revisada por la Comisión de Seguridad de la Información y Protección de datos personales siempre que se produzcan cambios relevantes en la información u organización del mismo. El contenido se adecuará en todo momento a las disposiciones legislativas vigentes en materia de seguridad de los datos de carácter personal, protegiendo adecuadamente la información conforme a la legislación mencionada.

En Guadarrama, a 27 de noviembre de 2023

Directora Gerente de Hospital Guadarrama



Rosa Salazar de La Guerra

ÍNDICE

INTRODUCCIÓN

Los avances en materia de Tecnologías de la Información que se están produciendo en los últimos años, sobre todo su amplia difusión entre el 2019-2021, han supuesto un amplio riesgo de vulneración de los Derechos Fundamentales de las personas titulares de datos personales.

La confidencialidad, integridad y disponibilidad puede verse gravemente amenazada por estos avances si no se realiza un adecuado uso de las tecnologías de la información y se incorporan los controles necesarios. En este contexto, quienes legislan han promulgado una serie de normas que tienen por objeto garantizar y proteger los datos personales también en el ámbito de la ciberseguridad.

La ciberseguridad es un compendio de diferentes normas relativas a la protección en internet, que hacen referencia en la misma a normativas de seguridad nacional, normativas de seguridad, normativas referidas a las telecomunicaciones, leyes sobre ciberdelincuencia, normativa de protección de datos y seguridad de redes y sistemas de información. La ciberseguridad son todas las medidas destinadas a la protección de los usuarios/as y empresas cuando operan en Internet, debiendo adoptar para ello diferentes medidas. Resumiendo: tenemos que aplicar una legislación adaptada a esta realidad:

- ✓ **Reglamento General de Protección de Datos (RGPD) de la Unión Europea, 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016,** en la que se establecen una serie de principios, obligaciones y procedimientos tendentes a garantizar y proteger los derechos de quienes ostentan la titularidad de los datos personales.
- ✓ **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)**, en la que se desarrolla el RGPD y se establecen una serie de principios, obligaciones y procedimientos tendentes a garantizar y proteger los derechos quienes ostenten la titularidad de los datos personales. Esta Ley contiene un título completo, el Título X, dedicado a la Garantía de los Derechos Digitales.
- ✓ **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)**, que tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos, garantizando adecuadamente la seguridad de la información tratada y los servicios prestados.

A partir de dicha legislación se han establecido distintas medidas a cumplir por todos los responsables del tratamiento, las cuales se pueden agrupar jurídicas, organizativas y técnicas.

1. OBJETIVO DE LA POLÍTICA DE SEGURIDAD

La presente Política de Seguridad tiene como objetivo describir el conjunto de directrices de índole organizativa y técnica que garantizan la confidencialidad, integridad y disponibilidad de la información contenida en los tratamientos con datos de carácter personal del Hospital, para así garantizar todos los derechos de las personas interesadas en cuanto a protección de datos y seguridad de la información.

2. MISIÓN DE LA ORGANIZACIÓN

El Hospital Guadarrama es un Centro público hospitalario, integrado en el Servicio Madrileño de Salud, de la Comunidad de Madrid.

El presente documento, en base a la legislación anteriormente citada, es aplicable a cualquier tratamiento de datos personales, ya sea en tratamientos automatizados o en soporte papel, tratados en el **HOSPITAL GUADARRAMA** (en adelante el Hospital).

En el ámbito personal: Todas las personas que tengan acceso a los datos contenidos en los tratamientos, bien a través de los sistemas informáticos, o bien en soporte papel, se encuentran obligadas a cumplir lo establecido en la presente Política de Seguridad, y están sujetas a las consecuencias que pudieran derivarse en caso de incumplimiento, incluso después de que esta relación se haya extinguido la misma.

En el ámbito funcional: Las medidas de seguridad que se adopten en este Documento son de aplicación tanto en las instalaciones propias del Hospital, como en cualquier otro lugar en el que se autorice el tratamiento de los datos sensibles parte de los tratamientos, tanto a personal del Centro, como a otras terceras personas mediante una relación contractual.

3. DEFINICIONES LEGALES

La terminología empleada en la presente Política de Seguridad hace referencia a las definiciones establecidas en el RGPD y la LOPDGDD. El glosario de términos se encuentra actualizado en INTRANET - GERENCIA- Protección de datos - PNT-PdD-01.

4. IDENTIFICACIÓN RESPONSABLES. DESIGNACIÓN Y RESPONSABILIDADES.

RESPONSABLE DEL TRATAMIENTO

NOMBRE	**HOSPITAL DE GUADARRAMA**
C.I.F.	**Q 2801270F**
DIRECCIÓN	**Paseo Molino del Rey, nº 2.** **28440 - Guadarrama. Madrid.**

RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

NOMBRE	COMITE DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCION DE DATOS DE CARACTER PERSONAL

RESPONSABLE DEL SISTEMA INFORMÁTICO

NOMBRE	**JUAN ANTONIO SANCHEZ GARCIA**

La designación formal para ocupar los cargos de Responsables se efectúa por la Persona Responsable del Tratamiento, en el seno de la Comisión de Seguridad de la información protección de datos personales y queda acreditada en el acta de dicha reunión. Lo mismo se procede a la hora de modificar la composición del Comité de Seguridad o los cargos de responsabilidad.

Las atribuciones de cada cargo responsable, así como mecanismos de coordinación y resolución de conflictos se reflejan en este documento.

CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD

El presente documento es de obligatorio cumplimiento para todos los que desempeñan un puesto de trabajo o colaboran en el centro.

Tanto el personal, propio o ajeno, relacionado con los sistemas de información están sujetos a lo dispuesto en esta Política de Seguridad, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicarán las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad de trabajo que serán aprobadas por el Comité de Seguridad de la Información y Protección de Datos Personales. Todas estas normas actualizadas están en:

Intranet – Gerencia – Protección de datos.

Las funciones y obligaciones del personal están descritas en el presente documento y en el PNT-PdD-02 Buenas prácticas en protección de datos que se encuentra en la Intranet.

ESTRUCTURA DE LA DOCUMENTACIÓN DE SEGURIDAD

1. El Comité de Seguridad será el encargado de aprobar el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles del Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
2. Como se indica en el apartado final, corresponde al Comité de Seguridad la revisión periódica de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte del Titular.

CENTROS DE TRATAMIENTO

El hospital cuenta con los siguientes centros de tratamiento:

➢ CENTRO DE PROCESO DE DATOS

En el CPD del Hospital se ubica el equipamiento sobre el que residen los Sistemas de Información para las áreas funcionales de Farmacia y Antivirus.

La dirección donde se ubican los Servidores que contienen las aplicaciones con información sensible, así como los puestos de trabajo del personal sanitario que manejan dicha información es:

Paseo Molino del Rey Nº 2. 28440 – Guadarrama. Madrid.

➢ **CENTRO TECNOLÓGICO Y CENTRO DE RESPALDO: CSCM - SIEMENS S.A.**

El Hospital Guadarrama accede a la Plataforma Asistencial SELENE gestionada por CSCM.

En el Centro Tecnológico se ubican todos los equipos que servirán de plataforma al Sistema de Información Centralizado MultiHospital, que permitirá el acceso a los datos desde cualquier ubicación. Este soporta toda la información de SELENE, AURORA, RIS/PACS, DATA WAREHOUSE, así como copia de los contenidos de todos los CPD's de los hospitales. La dirección de este CT es:

Hospital Universitario 12 de Octubre

El Centro de Respaldo está dotados con un equipamiento idéntico al del CT para los sistemas de información críticos y con la capacidad de almacenamiento suficiente para albergar el respaldo de los datos del CT y del CPD del Hospital. Esta información llega al CR a la par, es decir la información se genera de manera síncrona en ambos centros, con lo que se obtiene la redundancia de la información en tiempo real. La dirección postal del CR es:

Avda. Leonardo da Vinci, 15-19. Parque Empresarial La Carpetanía, Getafe. Madrid.

5. GESTIÓN DE RIESGOS

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad dentro del Hospital. La gestión de riesgos deberá realizarse de manera continua sobre los sistemas de información sanitaria, conforme a los principios de la seguridad basada en los riesgos, y reevaluación periódica, siendo el Comité de Seguridad de la información y Protección de Datos Personales, el encargado de que se realice el preceptivo análisis de riesgos y se proponga el tratamiento adecuado, determinando el nivel de riesgo aceptable y calculando los riesgos residuales.
2. El proceso de gestión de riesgos, comprenderá las fases de categorización de los sistemas, análisis de riesgos, la selección de medidas de seguridad a aplicar y la revisión post-implantación de dichas medidas. Para la implementación de estas medidas se deberá tener en cuenta los riesgos, el coste y la eficacia, es decir, que las mismas sean proporcionales a los riesgos, y que estén debidamente justificadas. Estas medidas, deberán ser útiles para minimizar los riesgos detectados, hasta alcanzar el nivel de riesgo aceptable definido por la organización. Ésta será una de las funciones de la persona responsable de sistemas informáticos, pasando posteriormente por el visto bueno del Comité de Seguridad, para la búsqueda de mejoras de forma continua.
3. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo, siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones realizadas por el Centro Criptológico Nacional.
4. Los análisis de riesgos, desde un enfoque de privacidad, se realizarán según lo establecido en la normativa vigente en materia de protección de datos personales, debiéndose seguir también las indicaciones de la AEPD y demás autoridades competentes al respecto.

6. MANUAL DE FUNCIONES Y OBLIGACIONES DEL PERSONAL

Las funciones y obligaciones del personal del Hospital con acceso a datos de carácter personal están establecidas en el presente apartado de la Política de Seguridad, incluyendo las funciones específicas en razón de la responsabilidad sobre la materia.

1. El personal del Centro no hará público los datos que conozcan como consecuencia o con ocasión del desarrollo de sus funciones correspondientes. Esta obligación subsistirá incluso una vez haya finalizado el vínculo con el centro. Además, en caso de incumplimiento estarán sujetos a las respectivas consecuencias disciplinarias, civiles y penales que procedan.
2. La Persona Responsable del Tratamiento (Dirección Gerencia) es quien decide sobre la finalidad, contenido y uso del tratamiento, y se encarga de implantar las medidas establecidas en este documento siendo también responsable de adoptar las medidas necesarias para que el personal con acceso a los datos personales conozca las normas al respecto.
3. Quien ostenta la responsabilidad de Seguridad es el Comité de Seguridad de la Información y Protección de Datos Personales, identificado en el Punto 4 es designado por la Persona Responsable del Tratamiento, y se encarga de coordinar, controlar y ejecutar las directrices organizativas, técnicas y funcionales necesarias para el correcto funcionamiento y cumplimiento de las medidas definidas en la Política de Seguridad, las cuales son de obligado cumplimiento. En cualquier caso, no tiene delegadas las responsabilidades que le corresponden a la Persona Responsable del Tratamiento.

4. Personal Administrador o personal informático: El personal que administra el sistema de acceso a los tratamientos de datos son:

- ✓ **Administradores/as** (Red, Sistemas Operativos y Bases de Datos). Tendrán la responsabilidad de los máximos privilegios y por tanto de máximo riesgo de que una actuación errónea pueda afectar al sistema. Tendrán acceso al software (programas y datos) del sistema, a las herramientas necesarias para su trabajo y a/o bases de datos necesarios para resolver los problemas que surjan.
- ✓ **Operadores/as** (Red, Sistemas operativos, Bases de Datos y Aplicación). Sus actuaciones están limitadas a la operación de los equipos y redes utilizando las herramientas de gestión disponibles. No deben, en principio, tener acceso directo a los datos del Fichero, ya que su actuación no precisa de dicho acceso.
- ✓ **Mantenimiento de los sistemas y aplicaciones.** Personal responsable de la resolución de incidencias que puedan surgir en el entono hardware/software de los sistemas informáticos o de la propia aplicación de acceso al Fichero.

OBLIGACIONES de las PERSONAS ADMINISTRADORAS DE SISTEMAS

- ✓ Gestión del de sistema operativo y de comunicaciones
- ✓ Gestión y control de los sistemas informáticos o aplicaciones de acceso los tratamientos de datos
- ✓ Salvaguarda y protección de las contraseñas personales
- ✓ Procedimientos de respaldo y recuperación
- ✓ Controles periódicos de verificación del cumplimiento

FUNCIONES Y OBLIGACIONES QUE AFECTAN A TODOS LOS USUARIOS/AS

Es todo el personal que utiliza normalmente el sistema informático de acceso a los tratamientos.

FUNCIONES Y OBLIGACIONES

- ✓ Confidencialidad y deber de secreto.
- ✓ Responsabilidad proactiva, comunicando incidencias que observen.
- ✓ Cumplimiento Obligatorio del Código de Buenas Prácticas ORDEN 1943/2005 de CSCM, y del resto de normativa vigente.

CONSECUENCIAS EN CASO DE INCUMPLIMIENTO

El incumplimiento de estas políticas puede dar lugar a que se tomen medidas disciplinarias, incluso al despido inmediato o al cese de otras relaciones con el Centro Hospitalario. Además, la infracción de cualquiera de la Funciones y Obligaciones impuestas al personal con acceso a los sistemas de información puede constituir también infracción de las leyes y dar lugar a la aplicación de sanciones civiles o penales (art. 197 y siguientes del Código Penal).

7. ESTRUCTURA Y DESCRIPCIÓN DE LOS TRATAMIENTOS

Están reflejados en el RAT y se podrán consultar en:

https://www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos

8. DESCRIPCIÓN DEL ENTORNO Y SISTEMAS DE INFORMACIÓN

ESQUEMA DE RED Y DE COMUNICACIONES HOSPITAL

El Hospital de Guadarrama cuenta entre sus instalaciones con diferentes infraestructuras:

- ✓ Edificio de Hospitalización
- ✓ Edificio anexo de Administración.
- ✓ Edificios anexos de Servicios (Lencería-Cafetería, Almacén y Mantenimiento)

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

El Centro de Proceso de Datos del Hospital donde se custodian los servidores que gestionan las aplicaciones e información sanitaria de pacientes se encuentra ubicado en la Planta 0 del Edificio de Hospitalización.

El Hospital está conectado por 9 bastidores RACK´S destinados a alojar los equipos informáticos, eléctricos y distribuidores de comunicación, los cuales son indispensables para conectar el sistema de información del Hospital (Hardware y Software) a la red de comunicaciones, garantizándose la disponibilidad de la información sensible clínico asistencial.

9. PROCEDIMIENTOS Y NORMAS DE CARÁCTER TÉCNICO

En el hospital Guadarrama se regulan todos los procedimientos de carácter técnico que se han adoptado e implantado en el Hospital para un adecuado uso de los sistemas de información según las exigencias de la normativa de protección de datos, así como para un correcto tratamiento de los datos de carácter personal en garantía de su confidencialidad e integridad. Con carácter general, son las siguientes:

- ✓ Normas relativas a las Aplicaciones
- ✓ Trazabilidad
- ✓ Normas relativas a los Equipos
- ✓ Disponibilidad
- ✓ Normas relativas a los Locales
- ✓ Acceso a datos a través de redes de comunicación
- ✓ Acceso remoto
- ✓ Sistemas de Seguridad de las líneas de comunicación

DELEGACIÓN DE AUTORIZACIONES

La Persona Responsable del Tratamiento puede delegar en otras personas la facultad de otorgamiento de autorizaciones que a él mismo le correspondan efectuar según lo indicado en el RD 1720/2007 y en este Documento. En el siguiente cuadro se hacen constar las personas habilitadas para otorgar estas autorizaciones, así como aquellas otras en las que recae dicha delegación.

En ningún caso esta designación supone una delegación de la responsabilidad que corresponde a la Persona Responsable del Tratamiento.

SaludMadrid Hospital Guadarrama — DELEGACIÓN DE AUTORIZACIONES			
Otorgante de la autorización	Responsable autorizado	Fecha	Finalidad de la autorización
Rosa Salazar de la Guerra Responsable del Tratamiento	Comité de Seguridad de la Información y Protección de Datos Personales	15/12/2016	- En caso de vacante, ausencia o enfermedad. - Autorizaciones de tratamiento fuera de los locales del fichero - Autorización de recuperación de datos - Autorización de acceso a la información o a los sistemas de información del Hospital a consultorías, empresas proveedoras, auditorías, personal externo. - Autorizaciones para el acceso a los tratamientos a las empresas de servicio de contratas para el mantenimiento de las aplicaciones. - Autorización de altas, bajas y modificaciones de usuarios/as. - Autorización para entrada y salida de soportes.

Comité de Seguridad de la Información y Protección de Datos Personales	Juan Antonio Sánchez García	15/12/2016	- Autorizaciones para la gestión de altas, bajas y modificaciones de usuarios/as. - Mantenimiento de datos, servidores o SAI y comunicaciones. - Autorización para gestión de soportes informáticos.
Comité de Seguridad de la Información y Protección de Datos Personales	Ángel Varela Álvarez	15/12/2016	Mantenimiento del SAI.
Responsable del Tratamiento	Ángel Varela Raúl Pompa	15/12/2016	Acceso por requerimiento de las fuerzas de seguridad a las grabaciones de las cámaras de videovigilancia

10. PROCEDIMIENTO NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS

Todas las incidencias relativas a aplicaciones y equipos informáticos son actualmente comunicadas por el personal afectado a la Persona Responsable del Departamento Informática para su resolución. Dichas incidencias son gestionadas y resueltas de forma interna en el Hospital. Únicamente si la incidencia afecta a los servidores del Hospital, el Responsable de Informática procede a contactar con HPCDS para su gestión y resolución.

En la Intranet – Gerencia – Protección de datos encontrarás el PdD-11 Gestión de incidencias de seguridad, con toda la información que necesitas.

1.1. Todo el personal del Hospital, así como los contratistas y terceros relacionados con la entidad deberán conocer los procedimientos para la comunicación de incidentes de seguridad establecidos por el Hospital, y en caso de detectar algún incidente, estarán obligados a comunicarlos al contacto designado.

1.2. Cuando ocurra un incidente que afecte a la seguridad de la información o a los servicios prestados, la persona afectada 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.

1.3. Los incidentes de seguridad deberán ser gestionados por el equipo de respuestas de incidentes, nunca por parte de la persona que los detecte. Dicho equipo, en cumplimiento de la normativa interna, deberá evaluar el incidente y comunicarlo 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.

1.4. La Persona Responsable de la Seguridad y/o el Comité de Seguridad del Hospital, que cuenten con competencias suficientes para ello, procederán, 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/a (incluyendo la retirada de los mismos), reportando esta acción, y su justificación, en cuanto sea posible, a los organismos implicados en el incidente.

11. CONTROL DE ACCESO LÓGICO

El sistema utilizado por el Hospital para limitar el acceso a las diferentes áreas del sistema en función de los privilegios de cada usuaria/o está descrito en el presente apartado de la Política de Seguridad y en el PNT-PdD.

11.1.1 PERFILES O GRUPOS DE ACCESO

Cada persona habilitada tiene acceso únicamente a la información que le permite el perfil que le ha sido asignado en relación con las funciones que le corresponda desarrollar según su puesto de trabajo o la actividad que le ha sido asignada en el Centro Hospitalario.

Los perfiles otorgados y los conjuntos de datos a los que puedan acceder han sido otorgados basándose en la función que realizan en el Hospital, estableciéndose con carácter general privilegios mínimos.

Los privilegios especiales o los perfiles con funciones más avanzadas, como creación de usuarios/as o asignación de las contraseñas iniciales, sólo se otorgan a quienes administran y a quienes realmente las necesiten en función de las tareas que se les hayan encomendado.

Las personas que no pertenecen al Hospital, como pueden ser personal de consultorías, empresas proveedoras, auditorías u otro personal externo, no tienen acceso a la información o a los sistemas de información del Hospital sin el permiso, previo y por escrito, de la Persona Responsable del Tratamiento. Cuando se requiera dicho acceso de terceros, hay que realizar una evaluación del riesgo para determinar sus implicaciones sobre la seguridad y las medidas de control que requieren. Estas medidas de control deben definirse y aceptarse en un contrato con la tercera parte.

Existe una relación de todo el personal con sus accesos autorizados a los sistemas de información del Hospital, así como una descripción de los perfiles o grupos de acceso definidos y privilegios asociados, responsables autorizados para acceder al repositorio y la gestión de la actualización de estos repositorios. La Persona Responsable de Seguridad se encarga de mantener actualizado este Anexo.

11.1.2 REGISTRO DE ACTIVIDAD Y DETECCIÓN CÓDIGO DAÑINO

1. Con el propósito de satisfacer el objetivo de la Política de Seguridad de Hospital, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados/as, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades del personal con acceso a los sistemas de información, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones Públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, las personas responsables de información podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la

distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

3. Para corregir o, en su caso, exigir responsabilidades, cada persona que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad. Ver en el PNT correspondiente, que se muestra en el siguiente punto.

11.1.3 GESTIÓN DE USUARIAS/OS

Para acceder a los sistemas de información que gestionan la información clínica asistencial de los/as pacientes, es indispensable en primer lugar estar dado de alta en el LDAP del Directorio Activo de CSCM, gestionado por el Centro de Soporte a Usuarios, Sistemas y Tecnologías de la Información (CESUS-ACCENTURE).

En concreto GESTIONAI, a través del *Módulo de Recursos,* posibilita de forma automatizada las siguientes acciones: Directorio Activo, correo electrónico, acceso a Internet y acceso a carpeta compartida. Además, a través del *Módulo de Aplicaciones,* posibilita de forma automatizada, las siguientes acciones, entre otras, SELENE.

Únicamente el personal autorizado en el presente procedimiento está habilitado para conceder, alterar o anular los accesos autorizados a los sistemas de información del Hospital, y según los criterios especificados a continuación.

En el PNT-PdD-07 Gestión de usuarios y contraseñas se detalla el procedimiento de alta y baja de usuarios y accesos.

11.1.4 IDENTIFICACIÓN Y AUTENTICACIÓN

Se han establecido procedimientos de identificación y autenticación para el acceso a los sistemas de información del Hospital mediante la introducción de un código de usuario/a y una contraseña. Ambos son las llaves de acceso a los sistemas, constituyen un componente básico de la seguridad de los datos y deben de estar especialmente protegidos.

Los códigos de usuario/a se han asignado al personal, así como también a otras personas que sin tener esa condición realicen actividades dentro del Centro Hospitalario por las que necesitan acceder a los sistemas de tratamiento de datos.

Algunos de los criterios generales para una correcta identificación y autenticación frente al sistema, que se han adoptado en el Hospital, son:

- ✓ La identificación de usuario/a (UserID) es personal e intransferible y es asignado una sola vez.
- ✓ No se reutilizan o reasignan códigos de usuario/a.
- ✓ Cada usuaria/o sólo tiene un código para acceder a un sistema único o a varios. Cada código de usuaria/o identifica a un usuario y no a un grupo, aunque los sistemas ofrezcan esta posibilidad.
- ✓ En los casos de necesitar compartir datos o correo se usarán otros mecanismos como carpetas o directorios públicos o sistemas de trabajo en grupo.
- ✓ Cada usuaria/o es responsable de la confidencialidad de su contraseña.
- ✓ Las contraseñas son almacenadas de forma ininteligible en los sistemas.

- ✓ Se asigna una única contraseña de acceso al sistema, y es el usuario el encargado de cambiarla en el primer acceso. En caso de ser necesario, la persona encargada de administrar el sistema invalida dicha contraseña.
- ✓ No se pueden establecer varias sesiones simultáneas por parte de un mismo usuario/a, salvo autorización expresa a determinados usuarios/as por la Persona Responsable del Tratamiento, y según función o necesidades técnicas en cada caso.

11.1.5 RESPONSABILIDAD DEL USUARIO/A

Los usuarios/as son responsables de todas las actividades y accesos que se realicen con su código de usuario/a y contraseña.

Todas las personas con permisos de acceso conocen las buenas prácticas en protección de datos que afecta a sus contraseñas.

Cualquier incidencia relacionada con los accesos restringidos, debe ser comunicada a la Persona Responsable de Seguridad, quien dejará constancia de la misma en el Registro de Incidencias correspondiente (Véase PNT-PdD-11 Gestión de incidencias de seguridad).

No se permite la creación de usuarias/as genéricos, ya que no permiten la correcta trazabilidad de las acciones desarrolladas por los usuarios/as en sus accesos a los sistemas de información. Ahora bien, se analizarán aquellas circunstancias excepcionales que se puedan dar en el Hospital y que requieran la implantación de este tipo de usuarios/as, siempre que el hecho pretendido y protegido sea superior a la vulneración producida de esta obligación de seguridad.

11.1.6 MÍNIMO PRIVILEGIO

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario/a.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

11.1.7 POLÍTICA DE CONTRASEÑAS

Las contraseñas de acceso al sistema son un pilar fundamental de la Protección de Datos, pues otorgan y garantizan confidencialidad en la información. Ver más en

INTRANET – Gerencia – Protección de datos – PNT-PdD-04 Creación y uso de contraseñas.

12. GESTIÓN DE SOPORTES INFORMÁTICOS

Los soportes informáticos son todos aquellos objetos físicos susceptibles de ser tratados en un sistema de información, medios de grabación y recuperación de datos que se utilizan para realizar copias o pasos intermedios en los procesos de la aplicación que gestionan los tratamientos de datos.

1. En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.
2. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.
3. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

12.1.1 IDENTIFICACIÓN E INVENTARIO

Cuando se necesite grabar datos de carácter personal en un soporte informático, previamente a su grabación, se debe etiquetar dicho soporte de forma diferenciada con el fin de distinguirlo de los demás soportes. La etiqueta contendrá una advertencia clara sobre el contenido del soporte y sobre la prohibición de acceso al personal no autorizado.

Siempre que los soportes contengan datos sensibles, como son los de salud e información clínica asistencial de pacientes, la identificación de los soportes se realizará utilizando un *sistema especial de etiquetado* comprensible y con significado que permita únicamente a los usuarios con acceso autorizado a dichos soportes identificar su contenido (ej. sistema de códigos de conocimiento restringido) y por lo tanto no sea posible que personas no autorizadas conozcan el contenido de dichos soportes.

Los soportes se deben guardar en un lugar protegido, con acceso restringido a personas no autorizadas. Dicho almacenamiento se realiza en locales o armarios bajo llave, estando el acceso a los mismos restringidos al usuario/a que lo creó o a las personas que deban conocer dicha información para proceder al desarrollo de sus funciones y que hayan sido expresamente autorizados por la Persona Responsable del Tratamiento.

Todos los soportes creados se recogen en un Libro de Inventario de Soportes, en el que se anotan consecutivamente, por cada copia realizada, la información que figura en la etiqueta de los soportes, añadiendo en su caso la fecha y el motivo de la baja, ya sea por destrucción o reutilización. El Inventario de Soportes actualizado está en manos de la Persona Responsable de informática.

La destrucción física del soporte dado de baja se realizará siguiendo el procedimiento de reutilización y destrucción de soportes de información. Véase el apartado siguiente.

12.1.2 DESTRUCCIÓN Y REUTILIZACIÓN

Cuando un soporte vaya a ser desechado o reutilizado, deben adoptarse las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en ellos, ya sea mediante borrado seguro, desmagnetización, cifrado, etc.

Dado que la mayor parte de los soportes son fácilmente transportables, reproducibles y/o copiables, es necesario adoptar las medidas de seguridad necesarias para evitar los riesgos contra la confidencialidad, integridad o disponibilidad de los datos.

12.1.3 DISTRIBUCIÓN DE SOPORTES Y TRANSMISIÓN DE DATOS

Cuando los soportes vayan a ser distribuidos, debe CIFRARSE su contenido o utilizar cualquier herramienta facilitada por el área de Informática que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

La información puede ser vulnerable a accesos no autorizados, sustracción, a mal uso o a corrupción durante su transporte físico. Con el objetivo de eliminar los anteriores riesgos se aplicarán algunos de los siguientes controles y medidas para salvaguardar los soportes informáticos transportados:

a) Deberían utilizarse transportes o mensajería fiable. Debería convenirse una lista del personal encargado de la mensajería con autorización un procedimiento para comprobar la identificación de los utilizados.

b) El envase debería ser suficiente para proteger el contenido contra cualquier daño físico que pueda ocurrir durante el tránsito, de acuerdo con las especificaciones de los fabricantes.

c) Deberían adoptarse controles especiales para proteger la información sensible, por ejemplo, Uso de contenedores cerrados, uso de firmas digitales, etc.

13. GESTIÓN DE DOCUMENTOS SOPORTE PAPEL

A pesar de la implantación de la infraestructura y modelo de gestión automatizado de información clínico asistencial, existe dentro de la organización del Hospital una serie de tratamientos de datos de usuarios efectuados en soportes papel, que suponen un riego a salvaguardar.

En este apartado se ponen de manifiesto las reglas que rigen la vida de todo documento soporte papel que contiene datos personales en el Hospital, desde que es creado hasta que es almacenado y finalmente destruido. Se puede ampliar esta información con el PNT PdD 10 Tratamiento de la información y su destrucción.

Las reglas y formas de actuación indicadas en el presente apartado son de obligatorio cumplimiento por parte de todo el personal que gestione o trate soportes en papel con datos personales e información clínica asistencial.

MEDIDAS DE SEGURIDAD

CREACIÓN

Para la creación de *documentos* se atenderá siempre al "*criterio de necesidad*", es decir, no se debe generar ningún documento en soporte papel que no sea necesario para el desarrollo de las funciones profesionales dentro del Hospital.

CLASIFICACIÓN DE DOCUMENTOS

El objetivo de la clasificación es posibilitar y facilitar la localización del documento por parte de la Persona Responsable del Tratamiento, así como garantizar el acceso al mismo y la respuesta al ejercicio de los derechos de Acceso, Rectificación, Cancelación, Oposición, Limitación, Olvido y Portabilidad (ARCOLOP) solicitados por los afectados en tiempo y forma.

La relación de los documentos existentes en el Hospital se lleva a cabo por la Persona Responsable del Servicio de Admisión y Documentación Clínica del Hospital, el Departamento de personal y Departamento de compras.

ALMACENAMIENTO Y CUSTODIA

Para garantizar la confidencialidad de la información, las carpetas que contienen documentos con datos de carácter personal son conservadas en armarios con llave u otra medida considerada análoga (puerta con llave, área no accesible al público, vigilancia permanente, etc.). Además, se tendrá control de Accesos por personal autorizado.

Conservación de Documentos: Los documentos solo deben conservarse el tiempo que dure la finalidad para la cual fueron creados. Ver en el PNT 10 la legislación aplicable a cada tipo de documento.
Destrucción de Documentos: La eliminación de documentos será efectuada de forma segura mediante máquinas destructoras u otros mecanismos similares que lleven a cabo la destrucción definitiva e impidan cualquier acceso no autorizado y recuperación posterior de la información.
Comprobaciones Periódicas: La Persona Responsable de Seguridad (Comité de Seguridad de la Información y Protección de Datos Personales) deberá realizar con una periodicidad como mínimo semestral, una comprobación del cumplimento de la presente política de gestión soporte papel.

PROCEDIMIENTO PARA ACCESO A HISTORIAS CLÍNICAS

La nueva legislación trata extensamente el tema de los derechos de los interesados en cuanto a protección de datos se refiere. En el Hospital están recogidos, en el PNT-PdD-13 (ver acceso más abajo) DERECHOS ARCOLOP, que es el acrónimo de los derechos de acceso, rectificación, cancelación, olvido, limitación, oposición y portabilidad.

Se parte de tres premisas:

- ✓ El acceso al contenido de la Historia Clínica es gratuito.
- ✓ El acceso podrá realizarse mediante copia o fotocopia.
- ✓ Queda limitado este derecho determinado supuestos.

Para ampliar la información ver:

INTRANET – Gerencia – Protección de datos - PNT-PdD-13 Derechos ARCOLOP.

SOLICITUD DE ACCESO CON FINES DE INVESTIGACIÓN Y DOCENCIA

Cuando la historia clínica es solicitada por personal sanitario del centro con la finalidad de investigación o docencia, el mismo presentará una solicitud donde informará de la investigación en marchar y las Historias en papel que necesita.

Con dicha autorización firmada por La Persona Responsable de información, la persona que lo solicita acudirá al Departamento de Admisión quien le proporcionará las Historias autorizadas durante máximo de dos meses.

GESTIÓN DE DOCUMENTACIÓN CLÍNICA EN PAPEL

En el ámbito de hospitalización existe un procedimiento muy exhaustivo (PNT-PdD-10) donde se definen los siguientes pasos:

- ✓ Búsqueda o apertura de historia clínica
- ✓ Generación de documentos iniciales a la H.C.
- ✓ Envío de documentación a planta y trabajo social.
- ✓ Custodia en la planta y trabajo social.
- ✓ Devolución a la unidad de documentación clínica para su archivo.
- ✓ Expurgo y archivo.
- ✓ Intranet – Gerencia – Protección de datos – PNT-PdD-10 Tratamiento de la información

SEGURIDAD Y CONTROL DE ACCESO FÍSICO

En el presente apartado se enumera un resumen de las medidas de seguridad relativas al control de acceso físico a las instalaciones del Hospital donde se encuentran ubicados los equipos informáticos que gestionan y tratan la información de pacientes, así como la información en papel de datos sensibles.

A través del control de acceso físico se pretende prevenir de forma efectiva el acceso indebido o no autorizado a las instalaciones por parte de terceros, a través de una serie de controles y barreras físicas, previniendo posibles intrusiones que pongan en riesgo la integridad y disponibilidad del equipamiento informático y, por lo tanto, mitigar los riesgos o amenazas de pérdida, alteración o divulgación de la información y de los datos almacenados en los equipos físicos protegidos, asegurando su integridad, disponibilidad y confidencialidad.

En el PNT-PdD-05 Normas de acceso y uso de la información podrán ampliar todo lo que desee.

Intranet – Gerencia – Protección de datos – PNT-PdD-05

Se incorpora información relativa a la seguridad física implantada en el Centro Tecnológico (CT) y Centro de Respaldo (CR) de SIEMENS S.A., donde se encuentra almacenada la información clínica de pacientes gestionada por la Plataforma Asistencial SELENE implantada por SIEMENS S.A. para CSCM.

INSTALACIONES GESTIONADAS POR SIEMENS S.A.

A continuación, se describen los controles y restricciones de acceso físico de SIEMENS S.A., en el Centro Tecnológico (CT) y Centro de Respaldo (CR) para garantizar la seguridad y el acceso restringido a dichas instalaciones donde se encuentran ubicados los equipos informáticos que dan soporte al Hospital y que almacenan datos sensibles de salud gestionados por la Plataforma Asistencial SELENE.

SEGURIDAD Y ACCESO FÍSICO

El control del acceso físico a las instalaciones donde se encuentran el CT y el CR se realizan desde la Recepción del edificio, custodiada por un guardia de seguridad que controla el ingreso tanto del personal laboral de la empresa como de las personas ajenas o externas a la organización. El personal de Recepción ha recibido formación específica en materia de protección de datos. El procedimiento a seguir está regulado.

SALAS CPD´S CENTRO TECNOLÓGICO Y CENTRO DE RESPALDO

Las salas de los CPD´s están dotadas de medidas de seguridad física y del entorno de carácter preventivo, así como de detección para garantizar la integridad de los equipos informáticos que soportan los sistemas de información y datos.

Las medidas de seguridad física y de entorno son las siguientes:

- ✓ Sistema de Circuito Cerrado de Televisión (CCTV).
- ✓ Sistemas de controles y equipamiento eléctrico
- ✓ Sistemas de Aire acondicionado conectados a grupos electrógenos
- ✓ Alarmas centralizadas en puesto de control principal de tal manera que personal de Seguridad y Mantenimiento actúen inmediatamente ante algún tipo de incidencia.

INSTALACIONES PROPIAS DEL HOSPITAL

➢ CONTRATACIÓN DE SERVICIOS DE SEGURIDAD

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación de la Política de Seguridad, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

➢ ACCESO A ZONAS CRÍTICAS

La protección puede lograrse creando una serie de barreras físicas en torno al Centro Hospitalario y a los recursos de tratamiento de la información. Cada barrera establece un perímetro de seguridad que aumenta la protección total.

La Persona Responsable de Seguridad (Comité de Seguridad de la Información y Protección de Datos Personales), velará por el cumplimiento de la reglamentación establecida, evitando el acceso de personal a zonas restringidas sin la autorización prevista, utilizando los medios disponibles a su alcance (cámaras de vídeo en circuito cerrado, puertas con clave de apertura, puertas esclusas o similares, alarmas, etc.). Comprobará, además, que los sistemas de seguridad funcionan correctamente, solucionando las posibles deficiencias que pudieran detectarse, y establecerá, si fueran necesarios, controles manuales, equivalentes a los automáticos, mientras durase la indisponibilidad del sistema de seguridad.

La entrada a la Sala de Servidores y Rack´s de Comunicaciones sólo está permitida al personal autorizado permanentemente, y a aquellas personas que por diferentes razones y de modo eventual se autorice esporádicamente su entrada, según se establece en los registros establecidos:

Hospital Guadarrama SaludMadrid

USUARIOS CON ACCESO AUTORIZADO

Doña Rosa Salazar de la Guerra, en su condición de Responsable de Fichero, y el Comité de Seguridad de la Información y Protección de Datos Personales, autorizan a los siguientes usuarios el acceso permanente a la Sala de CPD o Salas de Comunicaciones que dan soporte a los Sistemas de Información del Hospital:

Nombre y Apellidos	D.N.I.	Cargo/Empresa	Sala/s Autorizada/s	Firma del Responsable
Juan Antonio Sánchez García	50726397N	Responsable Dpto. Informática	CPDS y Armarios comunicaciones	
Ángel Varela Álvarez	71412993V	Jefe Mantenimiento	CPDS y Armarios comunicaciones	
Raúl Gómez	52504892D	Jefe de Seguridad	CPDS y Armarios comunicaciones	

Las visitas esporádicas a áreas seguras se supervisan, y se registra la fecha y momento de entrada y salida. Las visitas sólo tienen acceso para los propósitos especificados y autorizados, proporcionándoles instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia.

SEGURIDAD DE OFICINAS Y DESPACHOS

La Persona Responsable de Seguridad (Comité de Seguridad de la Información y Protección de Datos Personales), o la persona en quien delegue (Vigilante de Seguridad), velarán especialmente por el cumplimiento de la normativa de acceso y de permanencia en las dependencias de la entidad fuera del horario establecido.

SEGURIDAD Y CONTROL DEL EDIFICIO DEL HOSPITAL

Las instalaciones físicas del Hospital se encuentran ubicadas en:

Paseo Molino del Rey Nº 2. 28440 Guadarrama. Madrid.

La empresa contratada en el Hospital para la prestación de servicios de seguridad (Alerta y Control S.A.) y de videovigilancia (tiene el contrato de mantenimiento EMACS), con la cual se ha suscrito el correspondiente contrato de servicios y de encargo de tratamiento.

El Centro dispone de un sistema de vigilancia mediante monitorización de flujo de imágenes compuesto por unidades captoras de imágenes. El sistema de videovigilancia es monitorizado por personal de seguridad en el Centro de Control habilitado en el Hospital.

Se realiza un almacenamiento del flujo grabado de imágenes realizándose un autoborrado de los datos con una periodicidad máxima de 30 días.

Ante la solicitud por parte de los Cuerpos y Fuerzas de Seguridad de determinada franja de grabación, ver en

Intranet – Gerencia – Protección de datos - PNT-PdD-14 Requerimiento Fuerzas y Cuerpos de seguridad del Estado.

CONTROL DE ACCESO A LA SALA CPD HOSPITAL

El acceso a la sala del CPD sólo está permitido al personal autorizado previamente y de forma permanente por parte de La Persona Responsable del Tratamiento o persona delegada a tal efecto.

Toda persona con acceso esporádico autorizado al CPD debe estar acompañada y supervisada por personal con acceso permanente durante su acceso a la Sala hasta la salida de la misma; en cada una de las instancias se encuentra un documento que debe ser firmado por la persona autorizada que acceda, facilitando toda la información que se solicita.

El Centro de Proceso de Datos está dotado con alarmas de dos naturalezas distintas, dedicadas a la evaluación del correcto desempeño de los sistemas, emplazando en este grupo a los sensores que detectan una subida de temperatura y/o humedad por encima de los valores máximos tolerables, así como aquellos relativos al correcto suministro energético estabilizado mediante el sistema SAI.

Se encuentra instalado en el Hospital un grupo electrógeno propio generador de electricidad el cual se activa ante una caída de suministro eléctrico. Asimismo, cuenta con un equipo autónomo de aire acondicionado, conectado al grupo electrógeno principal del edificio de hospitalización.

SALAS DE RACK´S DE COMUNICACIONES

En el Hospital se encuentran distribuidos 7 bastidores (RACK´S) destinados a alojar equipos informáticos, electrónicos y distribuidores de comunicación, los cuales son indispensables para conectar el sistema de información del Hospital (hardware y software) a la red de comunicaciones, garantizándose la disponibilidad de la información clínica asistencial. Dichos RACKS están dotadas de puertas con acceso restringido a través de un sistema de apertura y cierre por llave.

PRUEBAS CON DATOS REALES

De acuerdo con la legislación en materia de protección de datos, no se emplearán datos reales en los entornos de pruebas y/o desarrollo, salvo que se garantice la seguridad de los mismos de acuerdo a su necesidad.

TELECOMUNICACIONES

La transmisión de datos sensibles a través de redes de telecomunicaciones se realiza **cifrando** dichos datos o bien utilizando cualquier otro mecanismo que garantiza que la información no es inteligible ni puede ser manipulada por terceros.

14. PRESTACIONES DE SERVICIOS POR TERCEROS

ENCARGO DE TRATAMIENTO

El Hospital comunica datos de carácter personal de sus tratamientos para el cumplimiento de fines directamente relacionados con sus actividades. Las empresas a quienes se comunican datos para la prestación de un servicio al Centro Hospitalario han firmado un contrato en el que se recogen todos los extremos exigidos de seguridad.

De conformidad a estos preceptos, el contrato de encargo de tratamiento debe cumplir unas exigencias que se recogen en:

Intranet – Gerencia – Protección de datos – PNT-PdD-03 Buenas prácticas para terceros

PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS

El Hospital adopta las medidas adecuadas para limitar el acceso a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Respecto a los contratos o convenios suscritos entre el Hospital y terceros que prestan servicios sin acceso a datos de carácter personal (limpieza, transporte, mantenimiento, voluntariado, etc.), dichos contratos deben de recoger la prohibición expresa de acceso a datos personales, así como la obligación de secreto respecto a los datos que hubieran podido conocer con motivo de la prestación de servicio. Todos estos contratos requieren la firma previa de la cláusula de confidencialidad.

15. CONTROL INTERNO DE VERIFICACIÓN DEL CUMPLIMIENTO

La veracidad de los datos contenidos en la Política de Seguridad y los procedimientos, así como el cumplimiento de las normas que contiene, son comprobados periódicamente.

Dichos controles periódicos serán realizados por el Comité de Seguridad de la Información y Protección de Datos Personales, el cual utilizará los criterios que considere adecuados para tal verificación.

Se registrarán dichos controles periódicos de verificación.

16. ACTUALIZACIÓN DE LA POLÍTICA DE SEGURIDAD

a) Por cambios que afecten su estructura o contenido:

   Siempre que se produzca un cambio que afecte a la estructura del Hospital, la Persona Responsable de Seguridad se encargará de actualizarlo realizando las modificaciones pertinentes.

   Si bien la responsabilidad de la actualización de la Política de Seguridad recae en la Persona Responsable de Seguridad, es necesario que los distintas Personas Responsables de Departamentos indiquen aquellas modificaciones que puedan afectar al mismo.

b) Por cambios de las disposiciones vigentes:

   Cualquier variación que se produzca y afecte a los aspectos contemplados en las disposiciones vigentes deberá recogerse de inmediato en la presente Política de Seguridad.

c) Actualización mínima:

   Con independencia de todo lo anterior, al menos una vez cada 3 años la Persona Responsable de Seguridad revisará el contenido de la Política de Seguridad y procedimientos y realizará los cambios pertinentes en los mismos.

   El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

17. DIVULGACIÓN DE LAS NORMAS DE SEGURIDAD

La Política de Seguridad está actualizada y a disposición de todo el personal en la Intranet del Hospital.

Intranet – Gerencia – Protección de datos

Para el correcto cumplimiento de la normativa de protección de datos se han desarrollado una serie de procedimientos para ampliar la información que también están disponibles y actualizados en la Intranet – Gerencia – Protección de datos. Son los siguientes:

- ✓ PNT-PdD-01 Glosario de términos
- ✓ PNT-PdD-02 Buenas prácticas en protección de datos
- ✓ PNT-PdD-03 buenas prácticas para terceros
- ✓ PNT-PdD-04 Creación y uso de contraseñas
- ✓ PNT-PdD-05 Normas de acceso y uso de sistemas de información
- ✓ PNT-PdD-06 Normativa compromiso confidencialidad
- ✓ PNT-PdD-07 Alta baja usuarios
- ✓ PNT-PdD-08 Copias de respaldo y recuperación
- ✓ PNT-PdD-09 Seguridad acceso internet
- ✓ PNT-PdD-10 Tratamiento información destrucción
- ✓ PNT-PdD-11 Gestión incidencias Seguridad
- ✓ PNT-PdD-12 Normativa uso correo
- ✓ PNT-PdD-13 Derechos ARCOLOP
- ✓ PNT-PdD-14 Requerimiento Fuerzas cuerpos de seguridad estado
- ✓ PNT-PdD-15 Captación tratamiento imágenes fines vigilancia

18. MODIFICACIÓN DE LA POLÍTICA Y PROCEDIMIENTOS

Tan solo la Persona Responsable de Seguridad, con la previa comunicación a la Persona Responsable del Tratamiento, podrá aprobar las modificaciones en los procedimientos incluidos en la Política de Seguridad. Las personas responsables de área podrán solicitar al mismo la modificación o inclusión de un procedimiento, para lo cual se comunicará el Comité de Seguridad de la Información y Protección de Datos Personales, mediante correo electrónico, la necesidad de la modificación o creación.

El Comité de Seguridad de la Información y Protección de Datos Personales será el que decida en reunión conjunta sobre la aprobación de dicha modificación, atendiendo a la operativa de trabajo y a las causas que motivan el cambio solicitado. Quedará reflejado en el Acta de la reunión.