Hospital Universitario Puerta de Hierro Majadahonda

Política de Seguridad

Comité de Seguridad de la Información

Ver	Fecha	Descripción	Autor(es)	Aprobado / Fecha
1.0	Agosto 2013	Versión Inicial	Comité Seguridad	Nov 2013
1.1	Octubre 2015	Actualización	Comité Seguridad	Comité de Seguridad
1.2	Junio 2017	Actualización	Comité Seguridad	Comité de Seguridad
2.0	Septiembre 2023	Actualización	Comité Seguridad	Comité de Seguridad

Comité de seguridad
25 de septiembre de 2023

Consideraciones de seguridad

Índice

1 INTRODUCCIÓN

El Hospital Universitario Puerta de Hierro Majadahonda (HUPHM) depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información tratada o los servicios prestados.

Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que se deban aplicar las medidas de seguridad exigidas por la legislación de Seguridad, así como realizar una evaluación de riesgos de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Esta Política de Seguridad de la Información se integrará en la normativa básica del HUPHM, incluyendo su difusión previa, y la instrumentación de las sanciones correspondientes por incumplimiento de la presente política, así como de los documentos relacionados a esta.

2 OBJETIVO Y MISIÓN DEL HUPHM

El Hospital Universitario Puerta de Hierro Majadahonda es un hospital de la red pública de la Comunidad de Madrid, cuya finalidad es prestar atención especializada de calidad a las personas, generando conocimiento y desarrollando investigación, todo ello encaminado a resolver los problemas de salud de la población.

Queremos ser un hospital de referencia asistencial, docente e investigadora a nivel estatal e internacional, reconocido por la sociedad y la comunidad científica por prestar una atención humanizada, segura, integral y altamente resolutiva, basada en el desarrollo profesional y la evidencia científica.

3 MARCO NORMATIVO

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

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.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS).

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Decreto 22/2008, de 3 de abril, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Sanidad.

ORDEN 491/2013, de 27 de junio, de la Consejería de Sanidad, 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.

4 ALCANCE

El alcance de la Política de Seguridad se centra en la información y los recursos de procesamiento de la información de todos los Sistemas de Información que usa, administra, o custodia el HUPHM.

5 DESTINATARIOS

La presente Política de Seguridad de la Información del HUPHM, será de aplicación y de obligado cumplimiento para todo el personal adscrito a él que, preste servicios en el mismo independiente de la forma de contratación y vinculación con el mismo, de manera permanente o eventual, que en el desempeño de sus funciones o parte de ellas desarrolle su trabajo fuera de sus instalaciones, en adelante los usuarios.

Será el Comité de Seguridad el encargado de la custodia y divulgación de la versión aprobada de este documento.

6 ORGANIZACIÓN DE LA SEGURIDAD

La estructura organizativa encargada de la gestión de la seguridad de la información en el ámbito de los sistemas de información y la administración electrónica del HUPHM, estará compuesta por los siguientes agentes: Comité de seguridad de la información, responsable de seguridad, responsable del sistema.

7 FUNCIONES COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El comité de seguridad de la información le corresponde aplicar, en el ámbito del HUPHM, las previsiones contenidas en el ENS, y ejercerá las siguientes funciones:

1. A nivel de gestión de la seguridad

- Implantación y seguimiento de las medidas preventivas y correctivas respecto de sus sistemas como resultado de los análisis de seguridad.
- Definir, revisar y modificar tanto la política, como el "Decálogo de buenas prácticas para usuarios de sistemas de información", cuando hubiere cambios en las tecnologías de la información y las comunicaciones, o en la organización.
- La aprobación del cuerpo normativo de seguridad que afecte transversalmente a toda la organización.
- Asumir las funciones del responsable de la información y del responsable del servicio, en los términos recogidos en el ENS.

2. *A nivel de coordinación de la seguridad*

- Impulsar nuevas líneas de trabajo en materia de seguridad de las tecnologías de la información y las comunicaciones, que conlleven la mejora continua del sistema de gestión de la seguridad de la información.
- Gestionar, coordinar y supervisar la seguridad de la información a nivel de organización. En concreto, dirigir las acciones en materia de seguridad de la información de los proyectos cuyo fin sea generar acceso electrónico a los servicios del HUPHM.
- Informar regularmente del estado de la seguridad de la información a la dirección.
- La definición de procedimientos internos y estándares respecto del ejercicio derechos SOPLAR por los pacientes y la provisión de información a pacientes y familiares.

3. *A nivel de control de la seguridad*

- La dirección y seguimiento de la aplicación de la legislación vigente, normas, estándares y buenas prácticas aplicables en materia de seguridad de las tecnologías de la información y las comunicaciones.
- El fomento de la formación y concienciación del personal en materia de seguridad de la información.
- El análisis de incidentes de seguridad ocurridos en el HUPHM y propuestas de mejora.
- Determinación de derechos de acceso a las aplicaciones por parte de los profesionales (definición de perfiles de acceso).

8 COMPOSICIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.

Presidente: Director Gerente del HUPHM.
Vicepresidente: Subdirector de Sistemas de Información.
Secretario: Delegado Protección de Datos del HUPHM.
Vocales:

- Representante de Informática o Sistemas de Información.
- Representante de Atención al Paciente.
- Representante de Dirección de Gestión.
- Representante de Recursos Humanos.
- Representante de Dirección Médica.
- Representante de Dirección de Enfermería.
- Representante de Admisión y Documentación Clínica.
- Representante del Servicio Juridico.

Invitados: a las reuniones del Comité podrá acudir, con voz, pero sin voto, convocados por el presidente, aquellas personas que, por razón de su actividad o conocimientos, tengan relación con los asuntos a tratar.

El comité se reunirá, previa convocatoria de su presidente y a iniciativa del mismo, como mínimo, una vez cada tres meses, y, con carácter extraordinario, cuando lo decida su presidente o lo soliciten la mayoría de sus miembros, y siempre que:

- Aparezcan incidencias de seguridad graves que afecten a cualquier ámbito de competencia de la Consejería de Sanidad.

- Surjan nuevas necesidades de seguridad que requiera la participación de los componentes del comité.

9 RESPONSABLE DE SEGURIDAD.

Tendrá las funciones y responsabilidades;

- Las funciones que le son propias como secretario del comité.
- Promover la seguridad de la información manejada y de los servicios prestados por los sistemas de información, así como la formación y concienciación de los usuarios en la materia.
- Llevar a cabo tareas de inspección mediante la realización de auditorías y controles periódicos, para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, por parte de las unidades y órganos que integran el hospital.
- Dirigir y coordinar la respuesta a los incidentes de seguridad, junto con otras unidades del hospital.
- Elaborar informes periódicos del estado de la seguridad de la información, en colaboración con las unidades y centros que la componen, para el comité, que incluyan los incidentes más relevantes de cada período.

Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el comité, a propuesta del responsable de seguridad, podrá designar responsables de seguridad delegados, en el número que considere necesario, que tendrán dependencia funcional directa del responsable de seguridad y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

10 RESPONSABLE DEL SISTEMA

El responsable del sistema será el titular del área o servicio del órgano competente en materia de sistemas de información y responsable de la explotación de los sistemas de información. Son funciones del responsable de sistemas:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Garantizar que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

11 DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

Las directrices de la Política de Seguridad serán desarrolladas de acuerdo a los estándares internacionales previstos en la ISO/IEC 27001:2005. Sistema de Gestión de Seguridad de la Información e ISO/IEC 27002:2009. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información, así como en el Esquema Nacional de Seguridad y Política de Seguridad de la Información de la OSSI. Todo ello, de acuerdo con la normativa en materia de protección de datos.

1. Organización e implantación del proceso de seguridad.

La seguridad de la información y protección de los datos de carácter personal deberá comprometer a todos los miembros del Hospital El Escorial. En el presente documento se identifican a los responsables de velar por el cumplimiento de la presente Política y ponerla en conocimiento de todos los miembros de la organización administrativa.

2. Análisis y Gestión de Riesgos.

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Este proceso comprende las fases de categorización de los sistemas y servicios, identificación de los activos, responsables, análisis de los riesgos y selección de medidas de seguridad a aplicar.

Este análisis de riesgos se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambien los sistemas y/o servicios prestados.
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves.

3. Gestión de Personal.

Todos los miembros del Hospital deberán ser formados e informados de sus deberes y obligaciones en materia de seguridad y protección de datos de carácter personal. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.

Su formación y concienciación será necesaria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

El significado y alcance del uso seguro del sistema se concretará y plasmará en las normas internas de seguridad del Hospital.

Será el Comité de Seguridad el encargado de fomentar la concienciación de los usuarios de los sistemas para alcanzar un grado de madurez en la formación seguridad de la información, por lo que deberá disponer de los medios necesarios para que la información llegue a los afectados.

Con la periodicidad establecida por el Comité y, al menos, una vez al año, se llevarán a cabo formaciones en aquellos temas que se haya detectado que se encuentran en mayor situación de olvido, o que por la criticidad de la información, es necesario incidir en la importancia de adoptar buenas prácticas en su tratamiento y custodia. Se establecerá un programa de concienciación continua para atender a todos los miembros del Hospital, en particular a los de nueva incorporación.

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros del Hospital y a todas las actividades, de acuerdo al principio de Seguridad Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

Así mismo, se definirán las exigencias de confidencialidad y no divulgación de datos para todos los miembros del Hospital, esta exigencia se definirá formalmente y todo el personal deberá firmar como prueba de recepción.

4. *Profesionalidad.*

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

El personal del Hospital recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios del Hospital.

5. *Autorización y control de los accesos.*

El acceso a los sistemas de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe 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 determinada actividad.

6. *Protección de las Instalaciones.*

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Por ello, en primer lugar se ha de establecer un perímetro físico de seguridad que proteja la información de la organización para prevenir incidencias, y garantizar el funcionamiento del resto de medidas.

El acceso a los locales, mediante vías de acceso autorizadas y controladas, barreras arquitectónicas como paredes o ventanas, elementos adicionales como áreas de descarga controladas, debe ser gestionado para proteger las zonas que contienen instalaciones informáticas o permiten el acceso a las mismas.

Dentro del perímetro de seguridad, se deben identificar las ubicaciones que almacenan soportes que puedan contener datos confidenciales o especialmente protegidos, estas ubicaciones dispondrán de una identificación personal de los usuarios que permita validar si disponen de autorización para su acceso.

Se deben validar las medidas de seguridad físicas de acceso al perímetro de seguridad, compuestas por puertas, cerraduras, alarmas, vigilancia,…y formalizarlas en instrucciones de acceso a los locales, que deberán ser comunicadas a todo el personal.

7. Adquisición de productos de seguridad.

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por el Hospital se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

La certificación indicada deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

8. Seguridad por defecto.

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean 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.

9. Integridad y actualización del sistema.

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

10. Protección de la información almacenada y en transito

En la estructura y organización de la seguridad del sistema, se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los siguientes dispositivos: equipos portátiles, tabletas, dispositivos periféricos, soportes de información (pen-drive, disco duro) y comunicaciones sobre redes abiertas o con cifrado débil.

Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por el Hospital en el ámbito de sus competencias.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

11. Prevención ante otros sistemas de información interconectados.

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, o a través de redes, con otros sistemas, y se controlará su punto de unión.

12. Registro de actividad

Con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que, de aplicación, se registrarán las actividades de los usuarios, 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.

13. Incidentes de seguridad

Deben registrarse los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema, y detección de vulnerabilidades. Se establecerá un sistema de detección y reacción frente a código dañino.

14. Continuidad de la actividad

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

15. Mejora continua del proceso de seguridad

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 gestión de las tecnologías de la información.

16. Proceso de revisión

La Política de Seguridad deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de administración electrónica, a la evolución tecnológica y al desarrollo de la información.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente Política, que se someterá, de haber modificaciones, a la aprobación del mismo.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

17. Terceros

Cuando el Hospital utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa,

pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.