USO INTERNO

POLÍTICA DE SEGURIDAD

DE LA INFORMACIÓN

HOSPITAL UNIVERSITARIO INFANTA CRISTINA

Datos sobre la presente edición

	Elaborado	Aprobado
Nombre	Jaime Gil	Carlos Mingo
Cargo	Jefe de Sistemas de Información	Comité de Seguridad de Sistemas de la Información
Firma		
Fecha	11.03.2015	11.03.2015

Nº de versión	Fecha	Resumen de cambios / comentarios
0.1	22.07.2014	Creación de Documento de Política de Seguridad del HUIC 2014.
0.2	11.03.2015	Modificaciones menores en varios puntos por el cumplimiento de la Norma UNE ISO/IEC 27001:2013.

Consideraciones de seguridad

La presente documentación es propiedad del HOSPITAL UNIVERSITARIO INFANTA CRISTINA y tiene carácter de USO INTERNO. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro. Asimismo tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito del HOSPITAL UNIVERSITARIO INFANTA CRISTINA, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguida conforme dicte la ley.

1 Índice

2 Introducción

HOSPITAL UNIVERSITARIO INFANTA CRISTINA 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, 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 mínimas de seguridad exigidas por la legislación de Seguridad, así como realizar un seguimiento continuo 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 a la normativa básica del HOSPITAL UNIVERSITARIO INFANTA CRISTINA, 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.

3 Objetivo

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Es esencial dar a conocer y concienciar a todo el personal, tanto interno como externo, que preste sus servicios en el HOSPITAL UNIVERSITARIO INFANTA CRISTINA sobre la estrategia de seguridad de la organización y definir las líneas estratégicas generales de actuación para evitar amenazas y reaccionar ante incidentes de seguridad.

La Política de Seguridad establece los principios básicos y requisitos mínimos de seguridad necesarios para proteger la información así como la tecnología utilizada para su procesamiento, estableciendo las directrices para la implantación de medidas organizativas, técnicas y legales y define los responsables de su desarrollo, implantación y gestión.

La implantación de dichas medidas se realizará de forma preventiva, reactiva, dinámica y mediante mecanismos de detección, que garanticen en todo momento la preservación de la información, y el cumplimento de las leyes en vigor que afecten a su uso y tratamiento.

La Dirección del HOSPITAL UNIVERSITARIO INFANTA CRISTINA adquiere el compromiso de velar por el cumplimiento de requisitos legales, reglamentarios, normativos y técnicos exigibles en materia de seguridad; así como de impulsar la mejora continua de su Sistema de Gestión de Seguridad de la Información.

4 Alcance

El alcance de la Política de Seguridad afecta a todo el Sistema de Gestión de la Seguridad de la Información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA y por tanto a toda la información y los recursos de procesamiento de la información que administra y/o custodia, independientemente del soporte (físico o lógico).

Asimismo, la Política de Seguridad cumple con las especificaciones del Esquema Nacional de Seguridad (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).

5 Destinatarios

La presente Política de Seguridad de la Información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA será de aplicación y de obligado cumplimiento para todo el personal del HOSPITAL UNIVERSITARIO INFANTA CRISTINA o 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.

La normativa de seguridad estará disponible en la intranet: HTTP://10.194.0.108.

6 Referencias y Marco Normativo

- 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.
- UNE ISO/IEC 27001:2015. Sistema de gestión de seguridad de la información.
- 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.

7 Contenido de la Política de Seguridad

El contenido de la presente Política trata de identificar, en primer lugar, a los responsables encargados de velar por la seguridad de la información y protección de datos de carácter personal del HOSPITAL UNIVERSITARIO INFANTA CRISTINA. Así mismo, en esta Política se contiene:

- Los objetivos en materia de seguridad que persigue el HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- El marco legal en el que se desarrolla su actividad.
- La estructura del Comité de Seguridad de Sistemas de Información, así como de la Unidad Independiente de Gestión de Seguridad, desarrollando su ámbito de responsabilidades, los miembros y la relación con otros elementos del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- Definición de las funciones de seguridad, definiendo por cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

8 Marco legal y regulatorio

En este apartado se recogen las normas más significativas correspondientes al ámbito de la seguridad de la información y la protección de datos:

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

- 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. BOE de 19 de enero de 2008.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica.
- 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.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE de 23 de junio de 2007.
- 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. BOE de 29 de enero de 2010.
- Ley 41/2002, de 14 noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

9 Organización de la seguridad en el Hospital

La estructura organizativa encargada de la gestión de la seguridad de la información en el ámbito de los sistemas de información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA, estará compuesta por:

9.1 Comité de Seguridad de Sistemas de Información.

El Comité de Seguridad de Sistemas de Información (en adelante, el Comité) es un órgano colegiado, cuya competencia será velar por e impulsar la seguridad de la información y protección de los datos de carácter personal del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.

9.1.1 Ámbito de responsabilidad.

El Comité se responsabiliza de alinear todas las actividades del HOSPITAL UNIVERSITARIO INFANTA CRISTINA en materia de seguridad de la información y protección de datos de carácter personal. En concreto:

- Coordina las actividades relacionadas con los sistemas de información y comunicaciones del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- Es responsable de la redacción de la Política de Seguridad de la Información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- Es responsable de la creación y aprobación de las normas que emanan del uso de los sistemas de información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- Aprueba los procedimientos de actuación y calificación en lo relativo al uso de los sistemas de información.
- Es responsable de velar por el correcto cumplimiento de las medidas de seguridad, en materia de protección de datos de carácter personal, de conformidad con lo establecido en el 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.

9.1.2 Funciones del Comité.

1. A nivel de gestión de la seguridad

- Elaborar la estrategia de evolución del HOSPITAL UNIVERSITARIO INFANTA CRISTINA. en lo que respecta a la seguridad de la información y protección de datos.
- Promover la mejora continua del sistema de gestión de la seguridad de la información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- Elaborar y revisar periódicamente, y al menos, una vez al año, la política de seguridad del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.

- Aprobar la normativa interna de seguridad de la información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA, así como su armonización respecto a la establecida por parte de la CSCM.
- Elaborar planes de mejora de la seguridad de la información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- Elevar los Planes de Contingencia a la Comisión de Dirección para su aprobación.
- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA de acuerdo con lo establecido en la Política de Seguridad de la Consejería de Sanidad.
- Elaborar procedimientos de Seguridad de la Información dentro de la actividad del HOSPITAL UNIVERSITARIO INFANTA CRISTINA, con la finalidad de implantar lo dictado en las normas de seguridad de la información de la CSCM.
- Analizar y proponer salvaguardias que prevengan incidentes similares en el futuro.
- Custodiar, mantener y actualizar el Documento de Seguridad conforme a el RDLOPD cuando se produzcan cambios o por indicación de los responsables de seguridad delegados.

2. A nivel de coordinación de la seguridad

- Coordinar la seguridad de la información a nivel de organización.
- Atender a las solicitudes e instrucciones del Comité de Seguridad de la Información de la CSCM.
- Coordinar los esfuerzos e interactuar con el Comité de Seguridad de la CSCM en todo lo referente a la seguridad de los sistemas de información.

3. A nivel de control de la seguridad

- Informar regularmente del estado de seguridad de la información al Comité de Seguridad de la Información de la CSCM.

- Impulsar planes de formación y concienciación en materia de seguridad de la información y protección de datos a todo el personal que preste sus servicios en el HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- Aprobar las medidas correctivas derivada de las Auditorias de Protección de Datos de Carácter Personal, y diagnóstico de seguridad de la información.
- Velar y supervisar la efectiva implantación de las medidas de seguridad necesarias en el desarrollo de todos los proyectos, desde su especificación inicial hasta su puesta en operación.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones respecto de ellos.

4. **El Comité asume la figura de Responsable de Seguridad, y con ello todas las funciones propias del mismo en materia de protección de datos, entre las que se encuentran:**

- Representar al HOSPITAL UNIVERSITARIO INFANTA CRISTINA, por delegación del Responsable del Fichero, en lo relacionado al cumplimiento de la normativa legal sobre el tratamiento de datos de carácter personal.
- Gestionar y coordinar la efectiva puesta en marcha de las medidas de seguridad, así como verificar cumplimiento de las mismas.
- Promover la difusión del Documento de Seguridad entre el personal del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- Revisará al menos de forma trimestral las incidencias registradas y propondrá las medidas correctoras que limiten su ocurrencia en el futuro.
- Solicitar periódicamente a los **responsables de seguridad delegados** (los cuales son definidos más adelante) que le reporten sobre el estado de implantación de las medidas de seguridad exigidas por la normativa de protección de datos de carácter personal.

9.1.3 Composición del Comité:

El Comité estará compuesto por los siguientes miembros:

1. **Presidente**: cargo que será ocupado por el titular de la Dirección Gerencial del HOSPITAL UNIVERSITARIO INFANTA CRISTINA, quien asumirá las siguientes competencia:

    - Convocar las reuniones periódicas del Comité.
    - Dirigir el Comité, proponiendo los distintos puntos a tratar en las reuniones periódicas.
    - Realizar el seguimiento de los distintos proyectos y equipos de trabajo que hayan surgido como respuesta a objetivos estratégicos y tácticos.
    - Comunicar al resto de comités de la CSCM las directrices claras a tener en cuenta en relación a los proyectos en curso y requisitos de seguridad que les puedan afectar.
    - Nombrar, a propuesta del Secretario, al resto de los miembros del Comité.

2. **Vicepresidente:** cargo que será desempeñado por Jefe de Servicio de Sistemas de la Información, quien desempeñara las funciones del presidente en ausencia de éste. Igualmente, será el Responsable de Seguridad del Fichero.

3. **Secretario:** podrá ser ocupado por el Jefe de Sección de Gabinete Jurídico del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.

    - Convocar las reuniones periódicas, así como las extraordinarias del Comité.
    - Preparar los temas a tratar en las reuniones del comité, aportando información puntual para la toma de decisiones.
    - Elaborar el acta de las reuniones.
    - Ser responsable de la comunicación directa o delegada de las decisiones del Comité.

4. **Vocales:**

    1. Representante de Atención al Paciente.
    2. Representante del área de Asesoría Jurídica.
    3. Representante de Recursos Humanos.
    4. Representante de Admisión y Documentación Clínica.

    Dichos representantes son nombrados por el presidente del Comité.

5. **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.

9.1.4 Delegación de funciones

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.

El Comité, en tanto en cuanto Responsable de Seguridad, designa diferentes Delegados, quienes se encargan de la efectiva implantación de las medidas fijadas por el Comité. En concreto:

Responsables de seguridad delegados de medidas organizativas:

1. **Representante de Recursos Humanos.** Cuyas funciones son:

    - Colaborar en la coordinación de las medidas de seguridad necesarias para los ficheros no automatizados, (soporte papel).
    - Facilitar a los usuarios de su área los medios para el correcto archivo, localización y conservación de información con datos personales.

- Establecer medidas para un correcto almacenamiento de la información con datos personales en armarios, cajones, archivadores u otros dispositivos que impidan su acceso por terceros no autorizados (por ejemplo, que tengan cerradura y llave).
- Para aquellos documentos o soportes con datos personales considerados información de especial sensibilidad (nivel alto), supervisa y verifica que se archiven en áreas o salas cerradas en las que el acceso esté protegido con puertas de acceso, dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente, que deberán permanecer cerradas cuando no sea preciso el acceso a dichos documentos o soportes.

2. **Representante de Atención al Paciente.** Cuyas funciones son:

- Se encarga de la gestión y tramitación de las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición que sean presentadas ante el HOSPITAL UNIVERSITARIO INFANTA CRISTINA. Al efecto, se encarga de la elaboración del registro de solicitudes de derechos ARCO, presentadas, contestadas (en plazo, fuera de plazo) y dar reporte de su situación al Jefe de Admisión del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- Mantiene actualizado el Documento de Seguridad en aquellos aspectos organizativos, relativos a medidas de seguridad aplicables a los sistemas de información no automatizados (soporte papel).

3. **Representante del área de Asesoría Jurídica.** Cuyas funciones son:

- Colabora en la confección, aportando su asesoramiento jurídico, de la normativa interna de Seguridad y Protección de Datos del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.
- Se encarga de la gestión y cumplimiento de las notificaciones que sean precisas de inscripción, modificación o supresión de los ficheros titularidad del HOSPITAL UNIVERSITARIO INFANTA CRISTINA ante el Registro de Ficheros de la Agencia Española de Protección de Datos.
- Asesora al Comité de Seguridad, en las cuestiones relacionadas con el cumplimiento de la normativa legal sobre el tratamiento de datos de carácter personal, verificando la existencia

de las cláusulas precisas en materia de protección de datos, así como la existencia de los Contratos de Encargo de Tratamiento de Datos con prestadores de servicios, así como documentos de cesión de datos a terceros, en su caso, entre otros.

- Colaborar en el análisis de los informes de auditoría desde el punto de vista legal.

4. **Representante de Admisión y Documentación Clínica.** Cuyas funciones son:

- Colaborar en la coordinación de las medidas de seguridad necesarias para los ficheros no automatizados, (soporte papel).
- Facilitar a los usuarios de su área los medios para el correcto archivo, localización y conservación de información con datos personales.
- Establecer medidas para un correcto almacenamiento de la información con datos personales en armarios, cajones, archivadores u otros dispositivos que impidan su acceso por terceros no autorizados (por ejemplo, que tengan cerradura y llave).
- Para aquellos documentos o soportes con datos personales considerados información de especial sensibilidad (nivel alto), supervisa y verifica que se archiven en áreas o salas cerradas en las que el acceso esté protegido con puertas de acceso, dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente, que deberán permanecer cerradas cuando no sea preciso el acceso a dichos documentos o soportes.

Responsable de seguridad delegado de medidas técnicas:

5. **Representante del área de Informática o Sistemas de Información.** Cuyas funciones son:

- Registra y controla las entradas y salidas en el HOSPITAL UNIVERSITARIO INFANTA CRISTINA de todos los conjuntos de información en sus diferentes soportes informáticos y documentos transmitidos vía telemática, y en especial todos aquellos que contengan datos de carácter personal, tal y como se contempla en el Documento de Seguridad.
- Realiza la carga, gestión y resolución de las incidencias relacionadas con el cumplimiento de las medidas de seguridad de la información y protección de datos personales, que

afecten a ficheros o tratamientos automatizados. Así como aquellas incidencias en materia de Seguridad.

- Custodia el Documento de Seguridad del HOSPITAL UNIVERSITARIO INFANTA CRISTINA y lo facilitará en caso de ser requerido por parte del Comité de Seguridad.
- Colabora en aquellos aspectos técnicos sobre los diferentes sistemas de información para la resolución, en las peticiones de ejercicio de derechos de acceso, rectificación, cancelación u oposición, a los datos personales (derechos ARCO).
- Verifica que la lista de usuarios autorizados se corresponde con la lista de usuarios con acceso real a los ficheros automatizados.
- Comprobar el correcto funcionamiento de los logs o registros de acceso a datos especialmente sensibles (nivel alto de medidas de seguridad) de los ficheros automatizados, con periodicidad al menos mensual, y elaborará un informe con las revisiones realizadas y los problemas detectados.
- Ejecuta las copias de respaldo que permitan la recuperación de los datos de los ficheros en caso de pérdida de los mismos.
- Implementa el registro de accesos a los CPD corporativos y a las salas de servidores de las distintas ubicaciones físicas del HOSPITAL UNIVERSITARIO INFANTA CRISTINA en su caso.

9.1.5 Funcionamiento.

El Comité se reunirá como mínimo cuatro veces al año y de forma extraordinaria, siempre que el Presidente lo considere pertinente, así como de forma inmediata tras un incidente de seguridad que afecte a la seguridad de la información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA, o a los datos de carácter personal custodiados por el mismo.

9.1.6 Elaboración del acta

Los temas que se adopten en las reuniones deberán estar alineados con la definición de los objetivos de seguridad que se traten de alcanzar dentro de cada plan de mejora de acciones

correctivas y preventivas, así como los objetivos por los cuales se constituye el Comité y las competencias que ostenta.

Después de cada reunión el Secretario levantará acta, que deberá ser firmado en todo caso, por el Presidente o el Vicepresidente.

Las actas contendrán:

1. Detalles de la Reunión: asistentes, convocatoria, fecha, convocante.
2. Lugar de reunión y asunto a tratar.
3. Resultado de las auditorias o revisiones de análisis de riesgos.
4. Estado de los planes de acciones correctivas, preventivas y en materia de formación.
5. Definición y asignación de los objetivos, concretos y cuantificables, en materia de seguridad de la información y protección de datos, así como análisis de su cumplimiento.
6. Técnicas y procedimientos implantados para mejorar la eficacia de la Seguridad.
7. Vulnerabilidad o amenazas no abordadas en el análisis de riesgos.
8. Resultados de las mediciones de eficacia.
9. Acciones de seguimiento de las revisiones anteriores.
10. Cambios que pudieran afectar a la gestión de seguridad de la información del Hospital.
11. Recomendaciones de mejora.

9.2 Unidad Independiente de Gestión de Seguridad

La Unidad Independiente de Gestión de Seguridad (en adelante, la Unidad) es el departamento interno del HOSPITAL UNIVERSITARIO INFANTA CRISTINA encargado de llevar a cabo un seguimiento del estado de la Seguridad de la Información. Está Unidad debe ser independiente del área de Informática o Sistemas de Información

9.2.1 Composición de la Unidad Independiente de Gestión

Las funciones de esta Unidad serán asumidas por el Comité.

9.2.2 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 27001:2013. Sistema de Gestión de Seguridad de la Información y el Código de Buenas Prácticas para la Gestión dela Seguridad de la Información, así como en el Esquema Nacional de Seguridad y Política de Seguridad de la Información de la CSCM. Todo ello, de acuerdo con la normativa en materia de protección de datos.

a) 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 UNIVERSITARIO INFANTA CRISTINA. 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.

b) Análisis y gestión de riesgos.

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, que deberán ser proporcionales a los riesgos y estar justificadas. De ser necesario, se elaborara un Plan de Tratamiento de Riesgos.

Este análisis 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.

Será el Comité de Seguridad el encargado de que se lleve a cabo el preceptivo análisis 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, las cuales serán reevaluadas y actualizadas periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

c) Gestión de personal

Todos los miembros del HOSPITAL UNIVERSITARIO INFANTA CRISTINA 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 UNIVERSITARIO INFANTA CRISTINA.

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 UNIVERSITARIO INFANTA CRISTINA, adecuados a cada puesto de trabajo, 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 UNIVERSITARIO INFANTA CRISTINA 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 UNIVERSITARIO INFANTA CRISTINA, esta exigencia se definirá formalmente y todo el personal deberá firmar como prueba de recepción.

d) 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 UNIVERSITARIO INFANTA CRISTINA recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.

Se hace necesario que, de manera objetiva y no discriminatoria, las organizaciones que presten servicios de seguridad al HOSPITAL UNIVERSITARIO INFANTA CRISTINA cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

e) 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.

f) 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.

g) 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 UNIVERSITARIO INFANTA CRISTINA 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.

h) 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.

i) 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.

j) 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 UNIVERSITARIO INFANTA CRISTINA 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.

k) 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.

l) 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.

m) Incidentes de seguridad

Todos los miembros de HOSPITAL UNIVERSITARIO INFANTA CRISTINA tienen la obligación de reportar incidentes o eventos que puedan afectar a la seguridad de la información.

Estos incidentes de seguridad deben registrarse, además delas acciones de tratamiento que se sigan. Todos estos registros se emplearán para la mejora continua del Sistema de Gestión de Seguridad de la Información del HOSPITAL UNIVERSITARIO INFANTA CRISTINA, y a la detección de vulnerabilidades.

Se establecerá un sistema de detección y reacción frente a código dañino.

n) 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.

o) 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.

10 Cuerpo Normativo

Las directrices de seguridad de la información indicadas en la presente Política de Seguridad se desarrollarán en un conjunto de documentos entre los que destacan, Políticas, Normativas, Guías, Procedimientos Operativos de Seguridad e Instrucciones de Trabajo.

La documentación sigue la siguiente estructura:

- El presente documento de Política de Seguridad del que emana el resto de documentos.
- Un documento de normativas que especifica los principios básicos y los requisitos mínimos de seguridad explicitados en el Esquema Nacional de Seguridad y enumera la relación de guías que es preciso desarrollar para lograr el cumplimiento de los citados principios básicos y requisitos mínimos de seguridad.
- Varios documentos guía donde se describe las actuaciones a desarrollar para implantar las medidas de seguridad enumeradas en el Esquema Nacional de Seguridad.
- Varios documentos de procedimientos operativos de seguridad, registros, instrucciones de trabajo, manuales, etc., que se desarrollan como consecuencia de aplicar las guías.

11 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 Comité de Seguridad del HOSPITAL UNIVERSITARIO INFANTA CRISTINA.

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.

12 Terceros

Cuando el HOSPITAL UNIVERSITARIO INFANTA CRISTINA utilice servicios de terceros o ceda información a terceros, se les hará participes 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.