POLITICA DE SEGURIDAD DE LA INFORMACIÓN

ÍNDICE Pg.:

1. OBJETIVO

El Departamento de Salud Valencia - La Fe depende de las Tecnologías de la Información y Comunicaciones para alcanzar sus objetivos de estrategia y operación. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a su disponibilidad, integridad, confidencialidad, uso previsto y valor de la información tratada o los servicios prestados.

El Departamento de Salud de Valencia La Fe, como consumidor de servicios y productos relacionados con los sistemas de información, participa en proyectos de diseño, desarrollo e implantación de los mismos, y por tanto también debe preocuparse de incorporar los controles adecuados desde las fases iniciales de los mismos.

El objeto del presente documento es la definición la Política de Seguridad de la información del Departamento de Salud Valencia - La Fe, dentro del alcance señalado en el Esquema Nacional de Seguridad y el Reglamento General Europeo de Protección de Datos, cumpliendo con todas sus especificaciones que son de aplicación. Esta Política de Seguridad de la Información se integra en la normativa básica del Departamento de Salud Valencia - La Fe.

La presente Política se ha definido atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas del Departamento de Salud Valencia - La Fe que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del 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).

El objetivo de la presente Política de Seguridad de la información es establecer los principios básicos y requisitos mínimos de seguridad necesarios para proteger la información, así como la tecnología utilizada para su procesamiento, así como garantizar la calidad de la información y la prestación continuada de los servicios.

Para ello, define directrices de implantación de medidas organizativas, técnicas y legales, desde la concepción del sistema y en todo su ciclo de vida hasta su desconexión y destrucción, y define los responsables de su desarrollo, implantación y gestión.

La implantación de dichas medidas se realizará de forma preventiva garantizando la preservación de la información, y el cumplimento de las leyes en vigor que afecten a su uso y tratamiento.

La presente Política de Seguridad de la información se debe dar a conocer a todo el personal, tanto interno como externo, que preste sus servicios en el Departamento de Salud Valencia - La Fe. Para ello se realizarán acciones específicas de formación y concienciación a todo el personal, y se instará a los encargados de tratamiento para que formen a los empleados que realicen tareas para el Departamento de Salud Valencia - La Fe.

2. 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 Departamento de Salud Valencia - La Fe.

La presente Política es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en el Departamento de Salud Valencia - La Fe, incluyendo, en su caso, el personal de proveedores externos, cuando accedan a los Sistemas de Información del Departamento de Salud Valencia - La Fe.

3. MARCO LEGAL Y REGULATORIO

Esta política está basada en las siguientes normas en el ámbito de la seguridad de la información, la protección de datos y la administración pública:

3.1. Protección de datos

- **Reglamento (UE) 2016/679**, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD).
- **Ley 3/2018,** de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales (LOPD y GDD).

3.2. Esquema nacional de Seguridad (ENS)

- **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.
- **Real Decreto 951/2015**, de 23 de octubre, de modificación del 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.
- **GUÍA DE SEGURIDAD (CCN-STIC-801)** Esquema Nacional de Seguridad Responsabilidades y Funciones.

3.3. Administraciones públicas

- **Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común** de las Administraciones Públicas, que señala en su art. 17.3 que los medios o soportes en que se almacenen documentos , deberán contar con las medidas de seguridad que establece el Esquema Nacional de Seguridad, que garanticen una serie de principios (como integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados); y, establece también, en su art. 27.3 que las Administraciones Públicas deberán cumplir con el Esquema Nacional de Seguridad para garantizar la identidad y contenido de las copias electrónicas o en papel, es decir, el carácter de copias auténticas.

3.4. Régimen disciplinario.

- **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público.
- **Ley 55/2003**, de 16 de diciembre, del Estatuto Marco del personal estatutario de los servicios de salud. Capítulo XII Régimen disciplinario.
- **Real Decreto Legislativo 5/2015**, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. Título VII. Régimen disciplinario.
- **Real Decreto 1146/2006**, de 6 de octubre, por el que se regula la relación laboral especial de residencia para la formación de especialistas en Ciencias de la Salud. Capítulo III Régimen disciplinario.

3.5. Políticas y roles

- **DECRETO 66/2012**, de 27 de abril, del Consell, por el que se establece la política de seguridad de la información de la Generalitat.
- **ORDEN 9/2012,** de 10 de julio, de la Conselleria de Sanidad, por la que establece la organización de la seguridad de la información (en adelante, Orden 9/2012).
- **Decreto 64/2018** del 18 de mayo que modifica el Decreto 610/2015 del 18 de septiembre del Consell por el que se aprueba el Reglamento orgánico y funcional de la Consellería de transparencia, responsabilidad social, participación y cooperación y en el Decreto 62/2018 de 18 de mayo del Consell de modificación del Decreto 103/2015 de 7 de julio del Consell por el que se establece la estructura orgánica básica de la presidencia y de las Consellerías de la Generalitat, se define la figura del Delegado de Protección de Datos y sus funciones.

4. PRINCIPIOS Y DIRECTRICES DE LA POLÍTICA

4.1. Principios para toda la organización

La seguridad de la información es un proceso que involucra a todos los miembros de la organización y a su interacción con procesos, tecnologías, materiales y ubicaciones físicas. También se involucran organizaciones externas, cuando tengan alguna relación de tratamiento de información o de acceso a sistemas de información.

Se implantará un sistema de gestión de la seguridad de los sistemas de información (SGSSI) alineado con las directrices del ENS, que preservará todas las dimensiones de la seguridad, a saber , Disponibilidad, Integridad, Confidencialidad, Trazabilidad y Autenticidad, para todos los activos relacionados con el tratamiento de información relevantes.

Los involucrados en tratamiento de información responderán de su seguridad, y colaborarán en la prevención, detección y control de los riesgos que atenten contra ella.

El SGSSI se guiará por los resultados de los procesos de análisis y gestión de riesgos de los distintos tratamientos.

El SGSSI incluirá un sistema de monitorización y mecanismos para la adaptación continua a los nuevos riesgos y nuevos métodos de protección.

Será misión del responsable del SGSSI la elaboración un informe sobre el estado de la seguridad, los riesgos valorados y los controles recomendados.

Será misión del responsable de la información y del responsable de tratamientos fijar el nivel de riesgo aceptable y ordenar la activación de los controles necesarios.

4.2. Principios para la explotación y operación de los sistemas

De acuerdo con el ENS, los principios y directrices que deben contemplarse a la hora de garantizar la seguridad de la información, durante la explotación de los sistemas que los tratan, **son la prevención, la detección, la respuesta y la recuperación**, para evitar la materialización de las amenazas existentes o, en caso de materializarse, minimizar su impacto en los servicios y la información afectada.

4.2.1. Prevención

El Departamento de Salud Valencia - La Fe debe prevenir, y evitar, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad, implementando las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Para garantizar el cumplimiento de la Política de Seguridad de la Información, los órganos directivos responsables deben:

- Autorizar los sistemas o los servicios antes de entrar en operación.
- Evaluar regularmente la seguridad, y cada vez que haya cambios de configuración.
- Programar revisiones por parte de terceros del cumplimiento del ENS.

4.2.2. Detección

Para prevenir la degradación de los sistemas y servicios, los órganos directivos responsables deben monitorizar la operación de manera continua para detectar y actuar en consecuencia.

En el supuesto de que la degradación sea atribuida a incidentes de seguridad, estos órganos directivos deberán establecer mecanismos de reporte que lleguen al responsable de seguridad.

4.2.3. Respuesta

Los órganos directivos responsables deben establecer mecanismos para responder eficazmente a los incidentes de seguridad.

4.2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, los órganos directivos responsables deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

4.3. Principios básicos para el diseño de sistemas

Adicionalmente, se establecen 7 principios básicos que deben orientar el diseño y desarrollo de sistemas y tecnologías que traten datos de carácter personal, y que engloban el principio de privacidad desde el diseño:

1. **Proactividad y prevención:** Los sistemas anticiparán y prevendrán eventos de invasión de privacidad antes de que estos ocurran.
2. **Privacidad por defecto:** en el diseño de los sistemas de información se asegurará que los datos personales estén protegidos automáticamente. No se requiere acción alguna de parte de la persona usuaria para proteger la privacidad.
3. **Privacidad Incrustada.** Las medidas que aseguran la privacidad estarán incrustada en el diseño y la arquitectura de los sistemas de Tecnologías de Información y en las prácticas del departamento de Salud. La privacidad se convierte en un componente esencial de la funcionalidad entregada, siendo parte integral del sistema.
4. **Funcionalidad Total.** En el momento del diseño se adaptarán todos los intereses y objetivos legítimos de manera que sea de utilidad para todas las partes interesadas.
5. **Seguridad Extremo a Extremo, en el Ciclo de Vida Completo**. La privacidad, Habiendo sido incrustada en el sistema antes de incorporar el primer elemento de información, se extiende con seguridad a través del ciclo de vida completo de los datos a tratar. En la implementación de sistemas de información se garantiza una administración segura del ciclo de vida del sistema, desde que se crea hasta que se desmantela.
6. **Visibilidad y Transparencia.** Con independencia de la tecnología y del proceso, se asegurará que todos los componentes del sistema permanecen visibles a usuarios y proveedores.
7. **Mantener un Enfoque Centrado en el Usuario y su privacidad.** Se requerirá a los arquitectos y operadores del sistema que mantengan en una posición superior los intereses de las personas, ofreciendo predefinidos de privacidad robustos, notificación apropiada, y facultando opciones de operación y ejercicio de derechos amigables

5. DESCRIPCION DE LA POLÍTICA

5.1. Tratamiento de datos de carácter personal

Para la prestación de los servicios de sistemas de información previstos en este departamento de salud deben ser tratados datos de carácter personal. Se implementará un Registro de Actividades del Tratamiento que detalla los tratamientos afectados y los responsables correspondientes, así como las medidas adoptadas derivadas de las evaluaciones de impacto realizadas sobre los tratamientos. Todos los sistemas de información se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro de Actividades del Tratamiento.

5.2. Desarrollo de directrices de Seguridad de la Información

Las directrices que deriven de esta Política de Seguridad se desarrollarán de acuerdo con la normativa en materia de protección de datos, el Esquema Nacional de Seguridad y la Política de Seguridad de la Información de la Conselleria de Sanidad Universal y Salud Pública.

5.3. Organización e implantación del proceso de seguridad

La seguridad de la información y protección de los datos de carácter personal debe comprometer a todos los miembros del Departamento de Salud Valencia - La Fe. En el apartado 6 de esta política 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.

5.4. Análisis y gestión de riesgos

Se definirá un proceso aplicable a todos los tratamientos de datos personales que 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.

El análisis se repetirá:

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

El Comité de Seguridad velará por 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.

El proceso de análisis de riesgos se realizará según las especificaciones del procedimiento **"1111-PG-067 Gestión del riesgo"**.

5.5. Desarrollo de la política

Esta Política de Seguridad de la Información será complementada mediante diversas recomendaciones de seguridad (políticas, protocolos, procedimientos, instrucciones técnicas, etc.) que se pueden consultan en nuestro sistema de gestión de seguridad de la información.

La Normativa de Seguridad está a disposición de todos los miembros de la Institución que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Está disponible para su consulta en http://intranetlafe.lafe.es.

5.6. Gestión de personal

Todos los miembros de Departamento de Salud de Valencia La Fe serán formados e informados de sus deberes y obligaciones en materia de seguridad y protección de datos de carácter personal.

La formación y concienciación será necesaria antes de asumir una responsabilidad, ya sea por primera asignación o por un cambio de puesto de trabajo o de responsabilidades en el mismo. Las actuaciones del personal serán supervisadas para verificar que se siguen los procedimientos establecidos.

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 se plasmará en las normas internas de seguridad del Departamento de Salud de Valencia La Fe.

El Comité de Seguridad pondrá los medios necesarios y se encargará de fomentar la concienciación de los usuarios de los sistemas para alcanzar un grado de madurez en la formación seguridad de la información.

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 Departamento de Salud de Valencia La Fe, 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 Departamento de Salud de Valencia La Fe 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 Departamento de Salud de Valencia La Fe. Esta exigencia se definirá formalmente y todo el personal debe firmar como prueba de recepción.

5.7. Profesionalidad

La seguridad de los sistemas será 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 Departamento de Salud de Valencia La Fe recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios.

Las organizaciones que presten servicios de seguridad al Departamento de Salud de Valencia La Fe, deberán contar con unos niveles idóneos de gestión y madurez en los servicios prestados.

5.8. Autorización y control de accesos

El acceso a los sistemas de información debe 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 estará identificado de forma única, quedando registro de su acceso, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

5.9. 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 establecerá un perímetro físico de seguridad que proteja la información de la organización para prevenir incidencias, y garantizar el funcionamiento del resto de medidas.

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

Dentro del perímetro de seguridad, se identificarán las ubicaciones que almacenan soportes que puedan contener datos confidenciales o especialmente protegidos. Para

acceder a estas ubicaciones, el personal dispondrá de una tarjeta de identificación con la que obtendrá la autorización de acceso.

Se validarán las medidas de seguridad físicas de acceso al perímetro de seguridad, compuestas por puertas, cerraduras, alarmas, vigilancia y se formalizarán en instrucciones de acceso a los locales, que serán comunicadas a todo el personal.

5.10. 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 Departamento de Salud de Valencia La Fe, se valoran positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

5.11. Seguridad por defecto y desde el diseño

Los sistemas se diseñarán y configuran de forma que garanticen la seguridad por defecto, en concreto se garantizará que:

- El sistema proporciona 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 son las mínimas necesarias, y se asegura que sólo son accesibles por las personas autorizadas, o desde emplazamientos o equipos, autorizados, incluyendo, si es el caso, restricciones de horario.
- En los sistemas en producción 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 de los sistemas ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

5.12. Integridad y actualización del sistema

Todo elemento físico o lógico requerirá por parte de la organización 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.

5.13. Protección de la información almacenada y en tránsito

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. Tienen 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.

Formarán parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por el Departamento de Salud de Valencia La Fe en el ámbito de sus competencias.

Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica, está 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.

5.14. Prevención ante otros sistemas de información interconectados

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entiende 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.

5.15. 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 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.

5.16. Incidentes de seguridad

Se registrarán 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 y se notificarán las incidencias, cuando proceda, al organismo competente según el procedimiento **1111-PG-068 “Gestión de incidentes y brechas de seguridad”.**

5.17. 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.

5.18. Mejora continua del proceso de seguridad

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

5.19. Cuerpo normativo: estructuración de la documentación de seguridad del sistema, su gestión y acceso

Estructuración de la documentación

Las directrices de seguridad de la información indicadas en la presente Política de Seguridad se desarrollan 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:

1. El presente documento de Política de Seguridad, del que emana el resto de documentos.
2. 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.
3. Varios documentos guía donde se describe las actuaciones a desarrollar para implantar las medidas de seguridad enumeradas en el Esquema Nacional de Seguridad.
4. Varios documentos de procedimientos operativos de seguridad, registros, instrucciones de trabajo, manuales, etc., que se desarrollan como consecuencia de aplicar las guías.

Gestión y acceso: Proceso de revisión, aprobación y difusión de la documentación

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

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 las novedades en el marco legal, infraestructura tecnológica, organización general, etc.

El Comité de Seguridad revisará la presente Política y toda la documentación de seguridad de la información, con periodicidad anual o cuando lo requieran las circunstancias, que se someterá, de haber modificaciones, a la aprobación del Comité de Seguridad del Departamento de Salud de Valencia La Fe.

El Comité de Seguridad del Departamento de Salud de Valencia La Fe se asegurará de que los documentos vigentes estén disponibles en la intranet: http://intranetlafe.lafe.es para todo aquel que lo necesite.

Para evitar el uso no intencionado de documentos obsoletos, el Responsable de Seguridad de la Información mantendrá actualizada una carpeta informática identificada

como “Obsoleto”, separada del resto de documentación, a la cual no tendrá acceso el resto de personal, siendo restringido el uso al Responsable del Seguridad de la Información.

Terceros

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes 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.

6. ROLES Y RESPONSABILIDADES

Los roles, responsabilidades y la estructura organizativa encargada de la gestión de la seguridad de la información en el ámbito de los sistemas de información del Departamento de Salud Valencia - La Fe se definen en el documento ***“1111-PG-69-Roles y responsabilidades”*** *que adapta lo indicado en* la Orden 9/2012, en el ENS y en la Guía de Seguridad CCN-STIC-801 ENS Responsabilidades y Funciones.

.Y está compuesta por:

6.1. Delegado de Protección de datos:

La figura del Delegado de Protección de Datos y sus funciones se define en la estructura orgánica básica de la presidencia y de las Consellerías de la Generalitat Valenciana (ver decretos 62/2018 y 64/2018 del Consell de la Generalitat Valenciana).

6.2. Responsable de los tratamientos de la información

La persona responsable de tratamientos de la información será la persona Responsable de Gerencia y encabezará la organización periférica de la seguridad de la información

en cada departamento de salud o instancia donde se establezca y actuará dentro de su ámbito en representación del responsable de la información.

6.3. Responsable local de la seguridad de la información

La persona responsable local de la seguridad de la información será la personal que ejerce las competencias de la Dirección Económica y desempeñará las funciones detalladas en el citado documento de roles y responsabilidades.

6.4. Responsable local de la seguridad de la información almacenada en ficheros automatizados

La persona Responsable local de la seguridad de la información almacenada en ficheros automatizados es la que ostenta la subdirección de los Sistemas de Información y desempeñará las funciones detalladas en el citado documento de roles y responsabilidades.

6.5. Responsable local de la seguridad de la información almacenada en ficheros no automatizados

La persona Responsable local de la seguridad de la información almacenada en ficheros no automatizados es y la persona Responsable de la Documentación Clínica y desempeñará las funciones detalladas en el citado documento de roles y responsabilidades.

6.6. Comité local de seguridad de la información

El Comité local de seguridad de la información es el máximo órgano consultivo de carácter no técnico sobre seguridad de la información en el Departamento. Se responsabiliza de alinear todas las actividades del Departamento de Salud Valencia - La Fe en materia de seguridad de la información y protección de datos de carácter personal.

Sus normas de funcionamiento, sus funciones, competencias y su composición están reflejadas en el documento de normas de funcionamiento, aprobado por la organización y publicado en la intranet del departamento de salud.

6.7. Responsables funcionales de tratamiento locales

Los responsables funcionales de tratamientos locales desempeñará las funciones detalladas en el citado documento de roles y responsabilidades, y son los siguientes perfiles:

- Responsable de Área de Docencia (Actividad formativa)
- Responsable de Área de Infraestructuras (Videovigilancia)
- Responsable de Área de Personal (Personal)
- Responsable de gestión económica (Actividad económica y gestión administrativa)

- Dirección médica (Información clínico asistencial)
- Dirección médica (Investigación clínica,sanitaria y farmacológica)
- Responsable de Área de Planificación (Organización y gestión de la actividad sanitaria)
- Responsable Área de Farmacia (Prescripción y dispensación farmacéutica)
- Responsable del área de seguridad y salud (Promoción de la salud,
- prevención del enfermad y salud laboral).

6.8. Responsables operativos de tratamiento

Cuando sea necesario esta función es asumida por la Dirección de Atención Primaria para todos los centros de salud del Departamento y por la Dirección Médica para los centros de especialidades y salud mental. Desempeñarán las funciones detalladas en el citado documento de roles y responsabilidades.

6.9. Responsable del servicio

Se ha designado responsables del Servicio a cada uno de los responsables de unidades funcionales, a quienes les corresponde las funciones descritas en el citado documento de roles y responsabilidades.

6.10. Responsable del Sistema

Se ha designado como Responsable del Sistema a la Subdirección de Sistemas de Información, quien asume las funciones descritas en el citado documento de roles y responsabilidades.

6.11. Administrador de seguridad del sistema:

Este puesto estará desempeñado por las personas Administradoras de comunicaciones, sistemas, aplicaciones y puestos que, como tal, le corresponden las funciones descritas en el citado documento de roles y responsabilidades.

6.12. Responsable de seguridad física

Este puesto estará desempeñado por la persona Responsable del Área de Hostelería (Seguridad y Vigilancia), y desempeñará las funciones que se especifican en el citado documento de roles y responsabilidades.

6.13. Responsable de gestión del personal

Este puesto estará desempeñado por la Subdirección de RRHH, y desempeñará las funciones que se especifican en el citado documento de roles y responsabilidades.

6.14. Procedimientos de designación de personas

La Dirección de la Organización, como responsable de los tratamientos, nombra formalmente a:

a) **Responsable de la Información**; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).
b) **Responsables del Servicio**; puede ser el mismo que el Responsable de la Información; puede ser un cargo unipersonal o un órgano colegiado (típicamente, el Comité de Seguridad de la Información).
c) **Responsable de la Seguridad**, que debe reportar directamente al Comité de Seguridad de la Información.
d) **Al Responsable del Sistema**, que debe reportar directamente al Comité de Seguridad de la Información.

La Dirección de la Organización designa al Administrador de Seguridad del Sistema a propuesta del Responsable del Sistema o del Responsable de Seguridad de la Información.

7. REGISTROS

El Comité Local de Seguridad es el encargado de la aprobación, custodia y divulgación de la versión aprobada de este documento. Cada cambio mayor aprobado será reflejado en el acta de reunión correspondiente.

Este documento y toda la normativa de seguridad vigente están disponible en la intranet del departamento de salud Valencia – La Fe cuya URL es http://intranetlafe.lafe.es

Cuando se produzca un cambio significativo en la estructura o en la operativa del Departamento de Salud Valencia - La Fe, si se ve afectada esta Política, deberá producirse una modificación y actualización del documento, siguiendo las directrices del procedimiento general de elaboración de procedimientos con la identificación 1111-PG-001, haciéndose una nueva versión del documento con los cambios y modificaciones identificados, y reflejándose en el apartado de control de cambios.