CONSORCIO
HOSPITAL GENERAL
UNIVERSITARIO
DE VALENCIA

EXTRACTO

Política de Seguridad de la Información

Consorcio Hospital General Universitario de Valencia

Documento	EXTRACTO. Política de Seguridad de la Información
Descripción	Documento que describe la Política de Seguridad de la Información del CHGUV
Fecha de creación	18/11/2019
Fecha de aprobación	7/5/2020

ÍNDICE

1 Aprobación y entrada en vigor

Texto aprobado el día 07 de mayo de 2020 por el Comité de Seguridad de la Información.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política. Será revisada, junto a las propuestas de revisión o mantenimiento de la misma, con una periodicidad mínima anual.

Con el objetivo de garantizar la calidad de la información y la prestación continuada de los servicios del hospital, el Hospital General Universitario de Valencia actúa de forma preventiva tomando las medidas adecuadas para proteger los sistemas frente a daños accidentales o deliberados, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Para defender los sistemas frente a las amenazas que ponen en riesgo su confidencialidad, integridad y/o disponibilidad se requiere una estrategia que implique a todo el personal que maneja la información del hospital.

Siguiendo los requisitos definidos por el Esquema Nacional de Seguridad, así como otras iniciativas de seguridad adicionales, se considera la Seguridad de la Información de una manera global en el hospital.

Por ello, se define la presente Política de Seguridad que se hace llegar a todo el personal para su conocimiento y cumplimiento. Tanto esta política como las normativas y procedimientos que de ella derivan serán revisados, actualizados y divulgados periódicamente para dar cabida a nuevos riesgos y amenazas y para mejorar de forma continuada la eficacia de los métodos de seguridad de la información aplicados.

2 Introducción

El Consorcio Hospital General Universitario de Valencia (en adelante, CHGUV), 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 o confidencialidad de la información tratada o los servicios prestados.

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.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. 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 las direcciones deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional 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.

Las diferentes direcciones deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por último, las direcciones deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1 Prevención

Las direcciones deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello las direcciones deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, las direcciones deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3 Respuesta

Las direcciones deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otras direcciones o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4 Recuperación

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

3 Alcance

Esta política se aplica a todos los sistemas pertenecientes al ámbito de las tecnologías de la información del CHGUV, abarcando todas las estructuras físicas y organizativas, así como a todo el personal del hospital, ya sea externo o interno, sin excepciones.

4 Misión del organismo

El CHGUV tiene como misión cuidar de la salud de la población, con la persona como referencia principal.

5 Objetivos

Con el fin de garantizar la protección efectiva de los recursos corporativos necesarios para el correcto funcionamiento del hospital, tanto de amenazas externas como internas y definiendo dicha protección en términos de calidad, se establecen los siguientes objetivos y principios básicos:

- Cumplir los requisitos legales y contractuales aplicables al desarrollo de sus funciones en el hospital, en especial, y a efectos de la presente Política, en las materias relacionadas con la protección de datos de carácter personal y con la continuidad de los procesos de negocio.
- Difundir entre todo el personal y hacer cumplir los procesos y normativa aplicables en materia de seguridad de la información, individualmente en función de sus tareas dentro del hospital.
- Restringir el uso tanto de la información en sí como de los sistemas que la procesan que son propiedad del CHGUV, a aquellas tareas necesarias para el correcto desempeño del trabajo de cada persona dentro del hospital; sin estar permitido el uso en beneficio particular de ningún activo.
- En el caso de la información, considerada como uno de los activos principales del CHGUV y que pertenece al propio hospital, es deber de todo el personal mantener el secreto respecto a la misma y no divulgarla a terceros, salvo que las comunicaciones formen parte de la relación laboral y en cumplimiento de las debidas garantías de confidencialidad.

6 Marco normativo y legal

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todo el personal del hospital que necesite conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la Intranet del CHGUV

Asimismo, el CHGUV se rige por el régimen jurídico recogido en el artículo 8 de la Resolución de 14 de julio de 2017, del director gerente del Consorci Hospital Universitari de València, por la cual se dispone la publicación de los estatutos refundidos del CHGUV.

Para dar cumplimiento a las necesidades identificadas dentro del marco del Esquema Nacional de Seguridad y directrices de la política antes mencionada, el Cuerpo Normativo de Seguridad que se deriva de la presente política se adapta a las necesidades y particularidades del CHGUV, derivadas de la regulación específica aplicable a su misión en su ámbito de actividad.

En el ejercicio de sus potestades públicas, será de aplicación la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En materia de protección de datos de carácter personal, el CHGUV cumple con lo dispuesto en la regulación aplicable:

- Reglamento General de Protección de Datos (Reglamento (UE) 2016/679).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

7 Obligaciones del personal

Todo el personal del CHUGV, interno o externo, tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad que la desarrolla, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Cuando se realicen acciones de concienciación en materia de seguridad de la información, el personal del CHGUV debe atenderlas, ya sea la lectura de materiales, comunicaciones (vía email, intranet, etc.), asistencia a sesiones presenciales, etc.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

Asimismo, queda bajo la responsabilidad de los usuarios hacer un uso proporcional, adecuado y justificado de los medios puestos a su disposición para el desarrollo de sus funciones. Cualquier uso indebido, podrá estar sometido al régimen disciplinario correspondiente dependiendo si se es funcionario o, personal estatutario (a los Funcionarios les será de aplicación el Real Decreto 33/1986, de 10 de enero, por el que se aprueba el Reglamento de Régimen Disciplinario de los Funcionarios de la Administración del Estado y, al personal Estatutario, el Estatuto Marco.)

8 Terceras partes

Cuando el CHGUV preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos comités de seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el CHGUV utilice 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 la normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias.

9 Documentación de Seguridad del Sistema

El sistema documental está formado por la presente Política de Seguridad, la Normativa de Seguridad y los procedimientos con código CHGUV-PR-XX, así como las instrucciones técnicas que derivan de ellos. Adicionalmente, puede que algunos procedimientos de otros grupos incluyan aspectos relacionados con los requisitos de seguridad marcados por el ENS.

Todos estos documentos se encuentran dentro del repositorio documental de Alfresco, accesible únicamente para el personal autorizado. En dicho repositorio se encuentran desde los documentos aprobados a aquellos que todavía permanecen en estado borrador.

La última versión aprobada se encuentra disponible en la intranet para todo el personal en modo lectura.

CONSORCIO
HOSPITAL GENERAL
UNIVERSITARIO
DE VALENCIA

Consorcio Hospital General Universitario de Valencia

Av. De las Tres Creus, 2, 46014 Valencia

T. (+34) 963 13 18 00

http://chguv.san.gva.es/