Política de Seguridad de la información edición Web

Hospital OCHOA

Noviembre de 2023

SISTEMAS		
Redactado	Revisado	Aprobado
Adrián Ramirez	Jose María Jimenez	Comité de Dirección

Versión	Motivo	Realizado por	Fecha
1	Creación del documento		14/11/2023

Contenido

1. Introducción

Este documento resume la Política de Seguridad de la Información del Hospital Ochoa como el conjunto de principios básicos y líneas de actuación a los que la organización se compromete, en el marco de las Norma ISO 27001.

La información es un activo crítico, esencial y de un gran valor para el desarrollo de la actividad de la organización. Este activo debe ser adecuadamente protegido, mediante las necesarias medidas de seguridad, frente a las amenazas que puedan afectarle, independientemente de los formatos, soportes, medios de transmisión, sistemas, o personas que intervengan en su conocimiento, procesado o tratamiento.

La Seguridad de la Información es la protección de este activo, con la finalidad de asegurar la continuidad del negocio, minimizar el riesgo y permitir maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información es un proceso que requiere medios técnicos y humanos y una adecuada gestión y definición de los procedimientos y en el que es fundamental la máxima colaboración e implicación de todo el personal de la empresa.

La dirección de la organización, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento.

Esta política ha sido aprobada por la dirección del **Hospital Ochoa** y se revisará anualmente.

2. Definiciones

Las **dimensiones** de la seguridad de la información son:

- **Disponibilidad:** Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.

- **Integridad:** La información del sistema ha de estar disponible tal y como se almacenó por un **agente**

- **Confidencialidad:** La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.

El **ciclo PDCA** es el que se utilizará durante todo el ciclo de vida del SGSI.

- **P (Planificar):** en esta fase se establecen las actividades, responsabilidades y recursos además de los objetivos a cumplir y cómo se van a medir estos objetivos.

- **D (Desarrollar):** se desarrollan los procesos y se implementan. Una vez implementados, hay que medir los resultados de la ejecución de dichos procesos.

- **C (Comprobar):** se analizan los resultados para comprobar si se han alcanzado los objetivos y si no es así, identificar las causas.

- **A (Actuar):** Se toman las acciones necesarias para corregir los fallos detectados en los procesos o para mejorarlos.

3. Requisitos legales y normativas

- 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.

- Ley 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

- Ley de Propiedad Industrial

- La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Las **normas** de referencia para la realización de los trabajos indicados, así como su ámbito de aplicación son las siguientes:

- Norma UNE-ISO/IEC 27001 Tecnología de la Información. Especificaciones para los Sistemas de Gestión de Seguridad de la Información, en la que se recogen los requisitos para establecer, implantar, documentar y evaluar un SGSI. Es la norma sobre la que se desarrolla el sistema y la que permite obtener la certificación de este por parte de un organismo certificador independiente.

- Norma ISO/IEC 27002 Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información. Esta norma ofrece recomendaciones para realizar la gestión de la seguridad de la información que pueden utilizarse por los responsables de iniciar, implantar o mantener la seguridad en una organización. Persigue proporcionar una base común para desarrollar normas de seguridad y constituir una práctica eficaz de la gestión.

4. Alcance

Los sistemas de seguridad de la información que dan soporte al servicio profesional médico quirúrgico proporcionado a sus clientes por Hospital

Ochoa Marbella S.L, así como Dermoestética Ochoa S.L. y Club Amigos Ochoa S.L., incluyendo todos los procesos administrativos de apoyo a todas las áreas del Hospital

5. Aplicación

La presente Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de la organización para los procesos descritos.

El personal sujeto a esta política incluye a todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre esta y de si el individuo es empleado o no de la organización. Por lo tanto, también se aplica a los contratistas o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la organización.

El contenido de la Política de Seguridad de la Información, cuando así se requiera, será desarrollado en normas y procedimientos complementarios de seguridad.

5. Propósito, Objetivos y Requisitos Mínimos de la Política de Seguridad

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información del **Hospital Ochoa.** Para ello se asegura la disponibilidad, integridad y confidencialidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente.

Es la política del **Hospital Ochoa** asegurar que:

- La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción.

- La confidencialidad de la información debe garantizarse de forma permanente, evitando el acceso y la difusión a toda persona o sistema no autorizado.

- La integridad de la información debe ser asegurada, evitando la manipulación, alteración o borrado accidentales o no autorizados.

- La disponibilidad de la información debe salvaguardarse de forma que los usuarios y sistemas que lo requieran puedan acceder a la misma de forma adecuada para el cumplimiento de sus tareas y siempre que ello sea necesario.

- Se establecerán planes de contingencia y continuidad para garantizar la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas y medios para su tratamiento.

- La Política de Seguridad de la Información es aprobada por la Dirección de la empresa y su contenido y el de las normas y procedimientos que la desarrollan es de obligado cumplimiento.

- Todos los usuarios con acceso a la información tratada, gestionada o propiedad de la empresa tienen la obligación y el deber de custodiarla y protegerla.

- La Política y las Normas de Seguridad de la Información se adaptarán a la evolución de los sistemas y de la tecnología y a los cambios organizativos y se alinearán con la legislación vigente y con los estándares y mejores prácticas de las normas ISO 27001 y Esquema Nacional de Seguridad.

- Se cumplen los requisitos legales aplicables.

- Se cumplen los requisitos del negocio respecto a la seguridad de la información y los sistemas de información.

- La Dirección valora los activos de información con los que cuenta el Hospital del cual derivará el análisis de riesgos y posteriormente la gestión de riesgos, tanto el análisis como la gestión de riesgos serán revisados anualmente por la Dirección, la cual decidirá si se efectúa un

nuevo análisis y gestión de riesgos. Los riesgos a tratarse se verán reflejados en el Plan de Seguridad.

- Las medidas de seguridad y los controles físicos, administrativos y técnicos aplicables se detallarán en el Documento de Aplicabilidad y la empresa deberá establecer una planificación para su implantación y gestión.

- Las medidas de seguridad y los controles establecidos serán proporcionales a la criticidad de la información a proteger y a su clasificación.

- Los usuarios que incumplan la Política de Seguridad de la Información o las normas y procedimientos complementarios podrán ser sancionados de acuerdo con lo establecido en los contratos que amparen su relación con la empresa y con la legislación vigente y aplicable.

- Las incidencias de seguridad son comunicadas y tratadas apropiadamente.

- Se establecen procedimientos para cumplir con la Política de Seguridad.

- El responsable de Seguridad será el encargado de mantener esta política, los procedimientos y de proporcionar apoyo en su implementación. Además de supervisar y comprobar que se cumpla el Plan de Seguridad que corresponda a ese año.

- La conformidad con las políticas de seguridad se justifica mediante la realización de auditorías internas según el procedimiento correspondiente.

Esta política de seguridad, se desarrollará aplicando los siguientes **requisitos mínimos**:

- **Organización e implantación del proceso de seguridad**: La seguridad deberá comprometer a todos los miembros de la organización.

- **Análisis y gestión de los riesgos** propio y proporcionado respecto a las medidas.

- **Gestión de personal**.

    - Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad.

    - Sus actuaciones deben ser 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 plasmará en unas normas de seguridad.

    - 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.

- **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

- **Autorización y control de los accesos**. El acceso al sistema 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.

- **Protección de las instalaciones**. Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

- **Adquisición y contratación de productos de seguridad**. En la adquisición o contratación de productos de seguridad de las tecnologías de la información y comunicaciones se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

- **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 alcance sus objetivos

    - 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.

- **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.

- **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.

  - Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

  - 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

- **Prevención ante otros sistemas de información interconectados**. El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas.

- **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 resulten 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.

- **Incidentes de seguridad**. Se establecerá un sistema de detección y reacción frente a código dañino. Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

- **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.

- **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.

6. Clasificación de la información

La información se clasificará de acuerdo a la sensibilidad requerida en su tratamiento y a los niveles de seguridad y protección exigibles.

7. Roles, Responsabilidades y deberes

La dirección asigna y comunica las responsabilidades, autoridades y roles en lo referente a la seguridad de la información. También se asegurará de que los usuarios conocen, asumen y ejercen las responsabilidades, autoridades y roles asignados.

Usuarios

Toda persona o sistema que acceda a la información tratada, gestionada o propiedad de la organización se considerará un usuario. Los usuarios son responsables de su conducta cuando acceden a la información o utilicen los sistemas informáticos de la organización. El usuario es responsable de todas las acciones realizadas utilizando sus identificadores o credenciales personales.

Los usuarios tienen la obligación de:

- Cumplir la Política de Seguridad de la Información y las normas, procedimientos e instrucciones complementarias.

- Proteger y custodiar la información de la organización, evitando la revelación, emisión al exterior, modificación, borrado o destrucción

accidental o no autorizadas o el mal uso independientemente del soporte o medios por el que haya sido accedida o conocida.

- Conocer y aplicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y el resto de políticas, normas, procedimientos y medidas de seguridad aplicables.

Propietario de activos de información

El propietario de un activo, entendiendo por tal al responsable de dicho activo, tendrá las siguientes responsabilidades:

- Definir si el activo está afectado por la Ley de Protección de Datos y aplicarle en su caso, los procedimientos correspondientes.

- Definir quiénes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación de la información y la función a desempeñar.

- Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del activo deberá informar a su vez al Responsable de Seguridad para tratar la incidencia.

- Informar al Responsable de Seguridad cuando ocurran cambios de personal que afecten al acceso de la información o los sistemas (cambio de función o departamento, causar baja en la entidad) para que se modifiquen apropiadamente los permisos de acceso.

- En los casos que aplique, asegurarse de que el personal y los contratistas tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

Dirección

La dirección de la organización está profundamente comprometida con la política descrita en este documento y es consciente del valor de

la información y del grave impacto económico y de imagen que puede producir un incidente de seguridad.

La dirección asume las siguientes responsabilidades:

- Demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información.

- Asegurar que se establecen la política y los objetivos de seguridad de la información y que estos son compatibles con la dirección estratégica de la organización.

- Aprobar y comunicar la Política de Seguridad de la Información, las Normas de Uso de los Sistemas de Información y la importancia de su cumplimiento a todos los usuarios, internos o externos, a los clientes y a los proveedores.

- Fomentar una cultura corporativa de seguridad de la información.

- Apoyar la mejora continua de los procesos de seguridad de la información.

- Asegurar que están disponibles los recursos necesarios para el cumplimiento de la política de seguridad de la información, de las normas de uso de los sistemas y para el funcionamiento del sistema de gestión de seguridad de la información.

- Definir el enfoque para el análisis y la gestión de los riesgos de seguridad de la información y los criterios para asumir los riesgos y asegurar la evaluación de los mismos al menos con una periodicidad anual.
- Asegurar que se realizan auditorías internas de seguridad de la información y que se revisan sus resultados para identificar oportunidades de mejora.

- Definir y controlar el presupuesto para seguridad de la información.

- Aprobar los planes de formación y las mejoras y proyectos relacionados con la Seguridad de la Información.

- Determinar las medidas, sean disciplinarias o de cualquier otro tipo, que pudieran aplicarse a los responsables de violaciones de seguridad.

Responsable de Seguridad

La persona con el cargo de Responsable de Seguridad Informática en el organigrama de la organización asumirá las siguientes funciones:

- Definir las políticas, normas y procedimientos de seguridad de la información e implantarlas tras la aprobación de la Dirección.

- Controlar el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.

- Gestionar y verificar los incidentes de seguridad y proponer medidas correctoras.

- Analizar y gestionar los riesgos relacionados con la seguridad de la información, determinar las vulnerabilidades y establecer las medidas de salvaguarda que garanticen la confidencialidad, integridad y disponibilidad de la información de acuerdo a un riesgo residual asumido por la organización.

- Proponer medidas y proyectos de mejora relacionados con la Seguridad de la Información a la Dirección para su aprobación.

- Elaboración y mantenimiento de los planes de contingencia y/o continuidad.

- Gestionar y supervisar el cumplimiento de la legislación vigente en materia de seguridad de la información incluyendo protección de datos, propiedad intelectual y sociedad de la información.

- Promover planes de formación, divulgación y concienciación en materia de seguridad de la información en la organización.

- Respecto a la protección de datos personales, asumirá el rol de Responsable de Seguridad LOPD-GDD y RGPD.

Comité de Seguridad de la Información

El comité de seguridad estará compuesto por

- El Responsable de Seguridad
- El Responsable del Sistema
- Un representante de la dirección
- A requerimiento, consultores o asesores en Seguridad de la Información y/o Protección de Datos personales

Se reunirá con una periodicidad trimestral y cuando sea requerido por alguna de las partes o en respuesta a incidentes graves de seguridad de la información. De estas reuniones quedará constancia en la correspondiente acta, y podrán derivarse acciones a implementar.

7. Evaluación de Riesgos de seguridad

Conocer los riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para la organización, ya que únicamente si se conoce el estado de seguridad podrán tomarse las decisiones adecuadas para mitigar los riesgos a los que se enfrenta.

Se utilizará la metodología Magerit para analizar los riesgos. Por ello, se realizará un análisis detallado de los riesgos que afecten a los activos recogidos en un inventario de activos, que quedará documentado en un documento de Análisis de Riesgos.

La entidad debe determinar los niveles de riesgo a partir de los cuales tomará acciones de tratamiento sobre los mismos. Un Riesgo se considera aceptable cuando implantar más controles de seguridad se estima que consumiría más recursos que el posible impacto asociado.

Una vez llevado a cabo el proceso de evaluación de riesgos, la dirección de la organización será responsable de aprobar los riesgos residuales y los planes de tratamiento de riesgo.

8. Proyectos

Todos los proyectos relacionados o que afecten a los sistemas de información deberán incluir, en su proceso de análisis, una evaluación de los requisitos de seguridad y definir un modelo de seguridad consensuado con el responsable de seguridad de la información.

En el diseño, desarrollo, instalación y gestión de los sistemas de información y en los proyectos se tendrán en cuenta y aplicarán los conceptos de seguridad desde el diseño, codificación segura y los controles y medidas de seguridad que proceda según el documento de aplicabilidad aprobado por la organización.

9. Contratación y adquisiciones

Todas las contrataciones y adquisiciones que supongan o requieran acceso o tratamiento de información clasificada como no pública, deberán realizarse amparadas por un contrato que incluya cláusulas destinadas a garantizar la salvaguarda de la confidencialidad, integridad y disponibilidad de información.

En aquellos casos en los que los servicios contratados supongan acceso o tratamiento por el proveedor de datos de carácter personal se deberá incluir en el contrato el clausulado requerido para el cumplimiento de la Ley Orgánica de Protección de Datos de Carácter Personal y Garantías de Derecho Digital, así como el Reglamento Europeo de Protección de Datos (RGPD).

Las organizaciones, empresas y personas que con motivo de contrataciones de servicios o adquisiciones de cualquier tipo accedan a información confidencial o de uso interno, deberán conocer la Política de Seguridad de la Información y las normas y procedimientos complementarios que sean de aplicación para el objeto de la contratación.

Las organizaciones, empresas y personas externas que accedan a la información de la organización deberán considerar dicha información, por defecto, como confidencial. La única información que podrán considerar como no confidencial es aquella que se haya obtenido a través de los medios de difusión pública.

10. Concienciación, Divulgación y formación

La presente Política de Seguridad de la Información debe ser conocida por todos los usuarios internos y externos y por las empresas que accedan, gestionen o traten datos de la organización.

El conjunto de Políticas, normas y procedimientos complementarios a esta

Política de Seguridad de la Información y el Documento de Seguridad LOPD-GDD también deberán ser adecuadamente comunicados y puestos en conocimiento de las personas, empresas e instituciones afectadas o implicadas en cada caso.

Se definirán, periódicamente, programas de comunicación, concienciación y formación y se entregará copia de la normativa correspondiente a los usuarios.

11. Respuesta a incidentes de seguridad

Cualquier compromiso de la confidencialidad, integridad o disponibilidad de la información de la organización se considera un incidente de seguridad.

Esto incluye, entre otros, el acceso, la eliminación, la destrucción, la modificación o la interrupción de la disponibilidad no autorizadas. También se consideran incidentes de seguridad los meros intentos de compromiso de las condiciones anteriores, los de evitar, alterar o modificar las medidas de seguridad o las violaciones o incumplimientos de la Política de Seguridad de la Información o de las normas y procedimientos complementarios.

Los usuarios son responsables de informar, de forma inmediata, de cualquier incidente de seguridad, a través de los canales y procedimientos definidos en la organización para la comunicación de incidencias.

12. Revisión y Auditorías

El responsable de seguridad revisará esta política anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la dirección.

Las revisiones comprobarán la efectividad de la política, valorando los efectos de los cambios tecnológicos y de negocio.