OFICINA DE SEGURIDAD DE LA INFORMACIÓN

CONCIENCIACIÓN EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN PARA PROFESIONALES DE G. A. S. DE SORIA

Sacyl | Junta de Castilla y León

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

1. IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR SANITARIO

Sacyl | Junta de Castilla y León

1.1. Importancia de la Seguridad de la Información en el sector sanitario

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

Información

ACTIVO ESENCIAL para proporcionar y prestar atención sanitaria. Gran volumen de datos.

DATOS SENSIBLES: de pacientes, datos de profesionales, datos de salud, historias clínicas, resultados de laboratorios, etc.

La información es **PROPIEDAD DE LA GRS**, y se utiliza para el cumplimiento de sus funciones asistenciales.

Qué proteger

CONFIDENCIALIDAD: la información no se debe poner a disposición, ni revelar a individuos, entidades o procesos no autorizados.

DISPONIBILIDAD: la información o los servicios deben ser accesibles siempre que sea necesario utilizarlos.

INTEGRIDAD: la información no se debe modificar o alterar de manera no autorizada.

Sacyl | Junta de Castilla y León

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

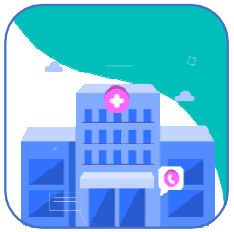
2. PRINCIPALES RIESGOS Y AMENAZAS DE SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR SANITARIO

Sacyl | Junta de Castilla y León

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

El sector sanitario como objetivo de ciberataques

Manejo de gran volumen de **datos sensibles y especialmente protegidos valiosos para los delincuentes.**

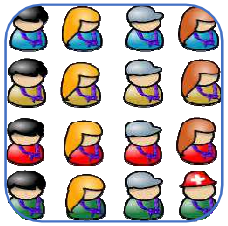


Múltiple y amplia superficie de exposición: Servicios operativos 24h x 365 días, centros físicos abiertos al público, aplicaciones tanto internas como expuestas en Internet, terceros con acceso a datos, etc.

Facilidad de engañar a los usuarios provechando las **situaciones de estrés** diarias.

Gran impacto reputacional dada la **regulación vigente**: RGPD, ENS, PIC, Ley de Autonomía del Paciente, etc.

Gran número de dispositivos obsoletos y/o no controlados difíciles de proteger: dispositivos médicos, dispositivos de gestión de hospitales, etc.



Gran **diversidad de perfiles profesionales** que tratan la información (celadores, médicos, técnicos informáticos, enfermeros, administrativos, etc.)

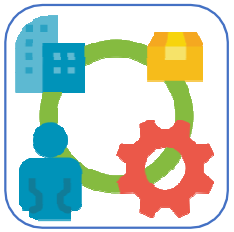
Sacyl | Junta de Castilla y León

2.2. Principales amenazas

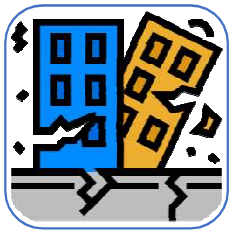
OFICINA DE SEGURIDAD DE LA INFORMACIÓN

Externas

CIBERATAQUES con diversas motivaciones: económicas, ideológicas, sabotaje, desestabilizar y causar daño en organizaciones y estados.



CADENA DE SUMINISTRO (proveedores): servicios, programas y dispositivos proporcionados por terceros y que pueden comprometer la seguridad de la GRS.



DESASTRES NATURALES: Incendios, terremotos, inundaciones.

Internas

PERSONAL INTERNO: falta de concienciación/formación, personal descontento, personal ajeno a la GRS con credenciales de acceso a sus sistemas.

ERRORES EN PROCESOS Y PROCEDIMIENTOS: ausencia de procedimientos operativos, fallos de diseño o incumplimiento de los mismos.

ERRORES EN CONFIGURACIONES DE SERVICIOS Y DISPOSITIVOS: contraseñas por defecto, funcionalidades activadas no necesarias, etc.

Sacyl | Junta de Castilla y León

2.3. Principales riesgos y amenazas en el sector sanitario - CASOS REALES - ESPAÑA

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

El Hospital Clínic de Barcelona sufre un ciberataque y deriva algunos servicios a otros centros

El ataque ha afectado a los servicios de laboratori… farmacia y urgencias

Hospital Clínic de Barcelona. Joan Manuel Baliellas EL MUNDO

El **Hospital Clínic de Barcelona** ha sufrido un ciberataque que ha obligado a derivar algunos servicios a otros centros hospitalarios, como parte de los servicios de urgencias o de transporte sanitarios.

Marzo 2023

Afectadas 800 máquinas virtuales y 31 servidores virtuales.
Filtrados 2.3TB de datos.
Paralizadas:
- **4000 analíticas.**
- **11000 consultas.**
- **300 intervenciones.**

SUBBÉTICA

Un ciberataque desvela miles de datos de pacientes y actividad clínica del Hospital Centro de Andalucía de Lucena

- La dirección del centro sanitario reconoce el "incidente de seguridad informática", al tiempo que asevera que no ha comprometido "el normal funcionamiento" del hospital

Enero 2022

Filtrados:
- **Historiales médicos de pacientes**
- **Datos administrativos**

SALUD · Los sistemas llevan cuatro días inutilizados

Torrejón, primer hospital español 'secuestrado' por un virus informático

El Hospital de Torrejón, en Madrid, lleva desde el pasado viern… con sus sistemas informáticos bloqueados por lo que parece se… un virus de tipo 'ransomware'.

Enero 2020

Bloqueo de todos los sistemas informáticos, incluyendo:
- **Acceso a los historiales clínicos**
- **Servicios de urgencias.**
- **Dispensadores de turnos**

Diario de Sevilla

SEVILLA

SEVILLA PROVINCIA ANDALUCÍA ESPAÑA ECONOMÍA SOCIEDAD DEPORTES CULTURA COFRADÍAS OPINIÓN TODAS LAS SECCIONES
SEVILLA VIVIR JUZGADO DE GUARDIA RUTAS DE SENDERISMO

ÚLTIMA HORA Muere en Sevilla la cantante María Jiménez
HACKEO El Ayuntamiento espera que los 'hackers' no tengan los datos de los sevillanos

DELITOS INFORMÁTICOS

Los hackers holandeses del ciberataque al Ayuntamiento de Sevilla piden hasta cinco millones de euros como resc…

- El grupo LockBit, de origen holandés, ha sido señalado com…
- "No vamos a ceder al chantaje"
- Los expertos ya advirtieron de que Sevilla era una de las pr… vulnerables a los ciberataques

Septiembre 2023

- **Han tenido que analizarse 4000 ordenadores y 800 servidores.**
- **Paralizados:**
  - **Padrón municipal**
  - **Pago de impuestos.**

Ataque de ransomware contra el hospital más importante de Asturias

- Al menos 200 personas pendientes de radioterapia en el Hospital Universitario Central de Asturias han visto cómo sus sesiones se han tenido que suspender

Diciembre 2021

200 pacientes vieron suspendida sus sesiones de radioterapia.

EL PAÍS

SANIDAD >

Detenida la falsa doctora que trabajó siete meses en el Hospital de Berga (Barcelona)

La mujer, que no tenía conocimientos de medicina, se hizo pasar por enfer… doctora en un mínimo de tres centros sanitarios

Según los Mossos, además del Hospital de Berga, hasta el… momento los investigadores también han podido confirm… la falsa doctora trabajó como enfermera y como médica … Hospital Universitario Dexeus de Barcelona y en una clín… Girona y que también formó parte del cuadro médico de una empresa de prevención de servicios sanitarios. La mujer elaboró y firmó informes y recetas con la firma digital de otro médico, utilizando su número de colegiado, según los Mossos, que

Julio 2023

Trató a 850 pacientes entre diciembre de 2022 y julio de 2022.

Sacyl | Junta de Castilla y León

2.4. Principales riesgos y amenazas en el sector sanitario - CASOS REALES - GRS

Febrero 2023

Sanidad frena ciberataques desde la India que pretendían robar identidades de los médicos

El intento de robo se produjo mediante 'phishing', pero desde la gerencia se señala que las medidas de seguridad funcionaron para evitar así el robo de datos de los profesionales y de los usuarios / El equipo informático de la Consejería de Sanidad logra frenar hasta diez ataques mediante phishing y refuerza la seguridad con un doble 'checking' con un código para los nuevos accesos de los sanitarios

Consultorio médico.-ICAL

Información relevante para pacientes proyecto ENEIDA

última actualización: 11 de julio de 2023 13:15

Julio 2023

GETECCU ENEIDA

Estimado/a paciente:

Desde la Sociedad Científica "Grupo Español de Trabajo en Enfermedad de Crohn y Colitis Ulcerosa (GETECCU)", en nuestra condición de Responsables del Tratamiento de Datos, nos ponemos en contacto con Usted para comunicarle una incidencia que ha afectado a información incluida en el Estudio Nacional en Enfermedad Inflamatoria Intestinal sobre Determinantes Genéticos y Ambientales (Proyecto "Eneida"), en el que se gestionan datos de pacientes con Enfermedad Inflamatoria Intestinal con fines estadísticos y científicos. Su centro hospitalario participa en dicho proyecto.

En este sentido, **el pasado miércoles, 14 de junio de 2023, nuestro proveedor tecnológico, Encargado del Tratamiento de Datos, detectó una incidencia de seguridad**, constatándose que se trataba de un ciberataque intencionado y doloso. De forma inmediata se establecieron las medidas necesarias para bloquear dicho ataque y se procedió a diseñar e implementar medidas adicionales de seguridad técnicas y organizativas. Al mismo tiempo, se procedió a comunicar la brecha de seguridad a la AGENCIA ESPAÑOLA DE PROTECCION DE DATOS en cumplimiento estricto de la normativa.

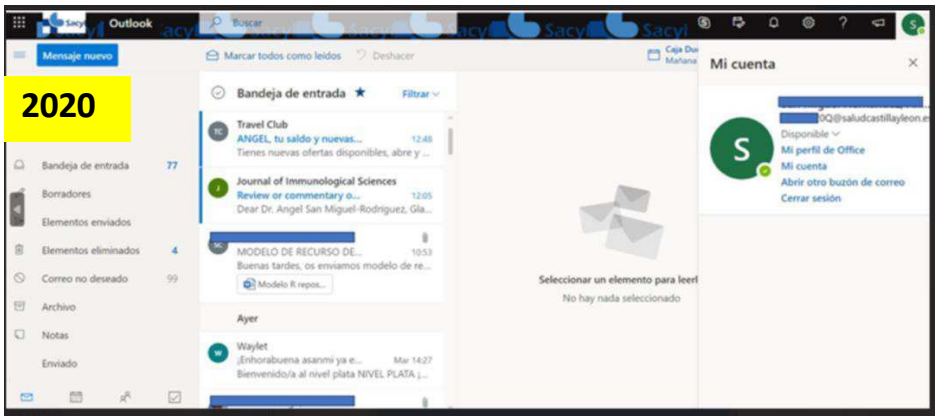
Entre la información sustraída, se encuentran **datos identificativos y datos de salud de pacientes del mencionado proyecto. Tras el análisis detallado llevado a cabo sobre el alcance del incidente, se ha constatado que, entre los**

Accesos a sistemas de la GRS con credenciales encontradas en la DarkWeb

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

2021

2020



Cotillear el historial clínico de los pacientes está penado.

Marzo 2023

Entrar en el programa de Sacyl para fisgar la historia clínica de un paciente con el que no hay relación asistencial deja rastro... y penas de más de dos años de prisión

Sacyl | Junta de Castilla y León

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

3. NORMATIVA APLICABLE

Sacyl | Junta de Castilla y León

3.1. Normativa aplicable

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

RGPD/LOPDGDD

Regulan el tratamiento de datos personales que hacen las organizaciones y confieren a sus titulares un mayor control sobre los mismos.

- **RGPD:** Reglamento europeo plenamente vigente y aplicable desde el 25 de mayo de 2018.
- **LOPDGDD:** Vigente desde el 7 de diciembre de 2018. Adapta al ordenamiento jurídico español lo dispuesto en el RGPD.

Principales implicaciones:

- Protección de datos desde el diseño y por defecto
- Bases de legitimación del tratamiento
- Principio de información y transparencia
- Figura del DPD
- Registro de Actividades del Tratamiento (RAT)
- Gestión de brechas de datos
- Evaluación de Impacto para la Protección de Datos (EIPD)
- Transferencias internacionales
- Encargados del tratamiento

LSSI/LGT

Regulan el régimen jurídico de los servicios de la sociedad de la información y de las telecomunicaciones.

- **LSSI**: Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- **LGT:** Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

Principales implicaciones:

- Obligación de informar mediante Aviso Legal en las páginas y sitios de Internet.
- Sanciones por infracción de la política de cookies.
- Deber de colaboración de los prestadores de servicios de intermediación.
- Obligaciones de información sobre seguridad.
- Prohibición de comunicaciones comerciales realizadas a través de medios de comunicación electrónicos.
- Infracciones por spam.

Sacyl | Junta de Castilla y León

3.1. Normativa aplicable

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

ENS

- **ENS: Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad**
- De aplicación a todo el Sector Público, así como a los proveedores que colaboran con las AAPP.
- Ofrece un marco común de principios básicos, requisitos y medidas de seguridad para una protección adecuada de la información tratada y los servicios prestados.
- **Objetivo**: asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos.

Principales implicaciones:

- Categorización de los sistemas (Básica, Media, Alta).
- Preceptivo análisis de riesgos.
- Aplicación del conjunto de medidas de seguridad según la categoría del sistema.
- Incorporación de la figura del perfil de cumplimiento.
- Protocolo de actuación ante ciberincidentes.

IC

- **Directiva 2008/114/CE**, sobre la identificación y designación de **infraestructuras críticas** europeas y la evaluación de la necesidad de mejorar su protección.
- **Ley 8/2011, de 28 de abril**, por la que se establecen medidas para la protección de las **infraestructuras críticas**.
- **Real Decreto 704/2011, de 20 de mayo**, por el que se aprueba el Reglamento de protección de las **infraestructuras críticas**.
- **Objetivo**: establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las AAPP.
- **¿Cómo?** Mediante la colaboración e implicación de los organismos gestores y propietarios de las infraestructuras.

Principales implicaciones:

- Instrumentos de planificación del sistema.
- Seguridad de las comunicaciones.
- El Responsable de Seguridad y Enlace.
- El Delegado de Seguridad de la Infraestructura Crítica.
- Seguridad de los datos clasificados.

Sacyl | Junta de Castilla y León

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

4. ESTRATEGIA DE LA GRS (PSIPD,NORMAS,PROCEDIMIENTOS, GUÍAS, ETC.)

Sacyl | Junta de Castilla y León

4.1. Estructura organizativa de seguridad de la GRS

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

La estructura organizativa encargada de la gestión de la seguridad de la información y protección de datos personales se encuentra definida en la PSIPD, en particular, en su artículo 7:

1. **Comité de Seguridad de la Información de la GRS.**
2. **Comisión Ejecutiva de Seguridad de la Información de los Servicios Centrales.**
3. **Comisiones Ejecutivas de Seguridad de la Información de las Gerencias de Asistencia Sanitaria (GAS), Gerencias de Atención Especializada (GAE) y Gerencias de Atención Primaria (GAP).**
4. **Roles de Seguridad esenciales.**

Responsable de la Información /Servicio

- Determina los requisitos (de seguridad) de la información

Responsable del sistema

- Mantiene el S.I. durante todo el ciclo de vida.
- Define la tipología y gestión de los S.I.
- Comprueba el estado de cumplimiento de las medidas de seguridad.

Responsable de la seguridad

- Coordina las medidas de Seguridad para satisfacer los requisitos establecidos por el R. de Información y el de R. Servicio.
- Relación directa con el CCN y CSIRT
- Promueve la formación en Seg. de la Información.

Responsable del Tratamiento

- Determina tanto la finalidad como los medios que se deben utilizar para el tratamiento de los datos personales.

Administradores de seguridad

- Aseguran la correcta implementación, gestión y mantenimiento de las medidas de seguridad aplicables a los sistemas de información.

Delegado de Protección de Datos (DPD)

- Se ha nombrado una única persona para toda la GRS.
- El DPD desempeña sus funciones con total autonomía, prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, y teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Sacyl | Junta de Castilla y León

4.2. Política de Seguridad y Protección de Datos (PSIPD, normas, procedimientos...)

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

PSIPD

Decreto 14/2023 de 21 de agosto, publicado en BOCYL 23/08/2023.
Regula el marco organizativo y de gestión aplicable a todos los sistemas de información y a todas las actividades de tratamiento de datos personales bajo la responsabilidad de la GRS.

De **obligado cumplimiento para todo el personal** que acceda a los sistemas de información o a la propia información de la GRS.
Tiene como alcance **todos los sistemas de información y actividades de tratamiento** responsabilidad de la GRS y de centros organismos adscritos a ella, independientemente del medio en el que esta se trate.

Principales procesos a gestionar:

- Análisis de riesgos (AARR).
- Evaluaciones de impacto en la protección de datos (EIPD).
- Gestión de riesgos.
- Auditorias de seguridad.
- Notificaciones de brechas de seguridad de datos personales.
- Formación y concienciación de los usuarios.

NORMAS, PROCEDIMIENTOS, GUÍAS, INSTRUCCIONES TÉCNICAS

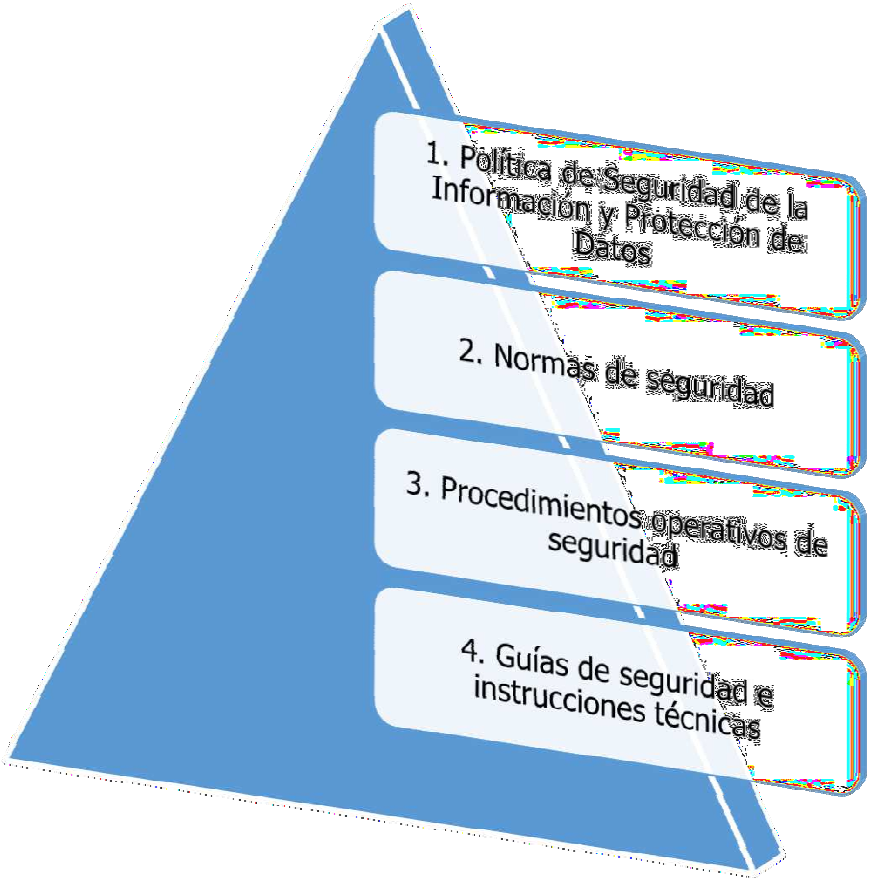
Normas: Detallan las medidas a implementar para asegurar la **seguridad integral**: gestión de personal, control de acceso lógico y gestión de contraseñas, seguridad física, protección de comunicaciones, adquisición, desarrollo y mantenimiento de sistemas, gestión de incidentes de seguridad, continuidad del negocio.

Procedimientos Operativos de Seguridad: **Documentos técnicos orientados a resolver tareas críticas**, con impacto en caso de una actuación inadecuada, sobre la seguridad, el desarrollo, el mantenimiento y la explotación de los sistemas de información.

Guías e instrucciones técnicas: **Documentos técnicos con recomendaciones y pasos a seguir** para la correcta implantación de medidas de seguridad sobre la infraestructura tecnológica que soporta la información y servicios de la GRS.

Sacyl | Junta de Castilla y León

4.3. Estructura documental y normativa



Categoría	Validado por	Aprobado por
Política	Comité de Seguridad de la Información	Alta Dirección de la GRS
Normas de seguridad*	Responsable de Seguridad de la Información	Comité de Seguridad de la Información
Procedimientos operativos de seguridad	Responsable de la Dirección Técnica	Responsable de la Dirección General competente en materia, previa validación por el Responsable de Seguridad de la GRS
Guías de seguridad e instrucciones técnicas	Responsable de la Dirección Técnica	Responsable de Seguridad de la GRS

*Publicadas en la Intranet del portal corporativo de la Gerencia Regional de Salud, en el plazo de 10 días desde su aprobación

4.4. Plan de medidas de seguridad en el acceso a adoptar por la GAS SO

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

- Cadenas de anclaje.
- Control de acceso físico a espacios comunes.
- Ordenadores con configuración autologon.
- Utilización de claves robustas.
- …
- …

Sacyl | Junta de Castilla y León

4.5. Código de conducta y buenas prácticas para profesionales

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

- Uso de equipos informáticos.
- Bloqueo de puesto de trabajo.
- Puesto de trabajo despejado.
- Uso de internet.
- Tratamiento y uso de datos personales.
- Protección de datos personales.
- Incidentes de seguridad.
- Uso de contraseñas.
- Uso de certificados digitales.
- Uso del correo electrónico.
- Uso de redes sociales.
- Transferencia de la información.
- Sistemas de almacenamiento de información en la nube.
- Finalización de vinculación con la GAS SO
- …

Sacyl | Junta de Castilla y León

OFICINA DE SEGURIDAD DE LA INFORMACIÓN

CONCIENCIACIÓN EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN PARA PROFESIONALES DE G. A. S. SORIA

Sacyl | Junta de Castilla y León