



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN ENS

Elaborado por: Responsable de Seguridad de la Información	Revisado por: Responsable de Servicio e Información	Aprobado por: Director General
Organización: Cambridge Business Initiatives S.L.	Organización: Cambridge Business Initiatives S.L.	Organización: Cambridge Business Initiatives S.L.
Fecha: 07/03/2024	Fecha: 05/08/2024	Fecha: 09/08/2024
Descripción: Política de Seguridad de la Información ENS		

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

CONTENIDO

1. INTRODUCCIÓN	3
2. MISIÓN	5
3. ALCANCE	6
4. MARCO NORMATIVO	6
5. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN	6
6. PREVENCIÓN	7
7. DETECCIÓN	8
8. RESPUESTA	8
9. RECUPERACIÓN	8
10. PRINCIPIOS	9
11. REQUISITOS MÍNIMOS DE SEGURIDAD	10
12. ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD	10
13. ANÁLISIS Y GESTIÓN DE LOS RIESGOS.....	11
14. GESTIÓN DE PERSONAL	12
15. PROFESIONALIDAD.....	12
16. AUTORIZACIÓN Y CONTROL DE LOS ACCESOS	12
17. PROTECCIÓN DE LAS INFRAESTRUCTURAS E INSTALACIONES	12
18. ADQUISICIÓN DE PRODUCTOS Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD	13
19. MÍNIMO PRIVILEGIO.....	13
20. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA	14
21. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO.....	14
22. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS	14
23. REGISTRO DE ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO	15
24. INCIDENTES DE SEGURIDAD.....	15
25. CONTINUIDAD DE LA ACTIVIDAD.....	16
26. MEJORA CONTINUA DEL PROCESO DE SEGURIDAD	16
27. CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS	16
28. ORGANIZACIÓN DE LA SEGURIDAD	17
29. COMITÉ DE SEGURIDAD.....	17
30. RESPONSABLE DE LA INFORMACIÓN	19
31. RESPONSABLE DE SERVICIO	20
32. RESPONSABLE DE SEGURIDAD.....	21
33. RESPONSABLE DEL SISTEMA	22

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

34. DELEGADO DE PROTECCIÓN DE DATOS	23
35. PROCEDIMIENTO DE DESIGNACIÓN.....	24
36. RESOLUCIÓN DE CONFLICTOS.....	24
37. DATOS DE CARÁCTER PERSONAL	25
38. GESTIÓN DE LOS RIESGOS.....	25
39. OBLIGACIONES DEL PERSONAL	27
40. TERCERAS PARTES	27
41. DESARROLLO Y ESTRUCTURA NORMATIVA	29
42. AUDITORÍA.....	30
43. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD	30

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

1. INTRODUCCIÓN

La Dirección de **Cambridge Business Initiatives S.L.** (en adelante, **SYGRIS**) identifica la seguridad y privacidad de la información como factores clave para la competitividad y sostenibilidad del negocio, así como para el cumplimiento normativo.

SYGRIS cuenta con un Sistema de Gestión de la Seguridad de la Información para garantizar la disponibilidad de los servicios que presta, la confidencialidad, integridad, trazabilidad y autenticidad de la información que maneja, implantando las medidas organizativas, técnicas y legales para proteger los activos del negocio.

La Dirección de **SYGRIS** ha establecido los procesos de planificación e implantación de los controles, salvaguardas y medidas de seguridad de la información, así como, de supervisión y mejora de la seguridad, con el fin de garantizar la confidencialidad, la integridad, la autenticidad y la trazabilidad de la información, así como de la disponibilidad de los servicios que se prestan a los clientes.

La Dirección de **SYGRIS** es responsable del Sistema de Gestión de Seguridad de la Información, como marco para el logro de los objetivos principales siguientes:

- Cumplir la legislación, en especial la de seguridad de redes y sistemas, la de protección de datos personales, la de propiedad intelectual e industrial y cualquier otra normativa que sea de aplicación
- Evaluar y tratar los riesgos de la seguridad y privacidad de la información
- Gestionar las incidencias de seguridad de la información
- Garantizar la continuidad del servicio
- Medir, analizar y optimizar los indicadores de eficacia y eficiencia de seguridad y privacidad de la información
- Mejorar los procesos de gestión y los controles de seguridad y privacidad de la información.
- Supervisar, auditar y acreditar la conformidad con la norma ISO/IEC 27001 y el Esquema Nacional de Seguridad.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

La Dirección de **SYGRIS**, para la implantación, mantenimiento, supervisión y mejora del Sistema de Gestión de Seguridad de la Información ha tomado las decisiones siguientes:

1. Constitución de un Comité de Seguridad de la información como órgano colegiado superior para la supervisión, coordinación y toma de decisión en materia de seguridad y privacidad de la información
2. Designación de los Responsables del Servicio, de la Información, de Seguridad de la Información y del Sistema de información
3. Designación de un Delegado de protección de datos
4. Analizar y tratar los riesgos de la seguridad y privacidad de la información derivados de la prestación de servicios e implantar los controles, las medidas o las salvaguardas necesarias para su mitigación, transferencia o eliminación.
5. Asignación de los recursos personales y materiales para satisfacer los requisitos de seguridad de la información, manteniendo el equilibrio entre coste y beneficio.
6. Concienciar y formar a todo el personal y colaboradores, en materia de riesgos y amenazas a la seguridad de la información y en las medidas a seguir para su prevención y mitigación o, en su caso, en la notificación de incidencias.
7. Implantación de las medidas apropiadas para garantizar los niveles de seguridad de la información de los componentes y servicios contratados, previniendo, respondiendo y resolviendo las incidencias que puedan producirse.
8. Medir y analizar los objetivos e indicadores de seguridad de la información que permitan a la Dirección el seguimiento de los riesgos e incidencias de seguridad, así como de las actividades de control.

La presente política se complementa con el resto de las políticas, procedimientos y documentos en vigor del Sistema de Gestión de Seguridad de la información de **SYGRIS**.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

2. MISIÓN

La misión de Sygris es simplificar, optimizar y digitalizar los procesos ESG corporativos, abordando los retos de capturar, gestionar y trazar la información no financiera de las empresas, asegurando el cumplimiento de la normativa vigente gracias a nuestra tecnología, diseñada específicamente para el tratamiento de datos ESG.

Los sistemas de información de **SYGRIS** deberán ser gestionados con diligencia, implantando las medidas necesarias para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad de la información tratada y/o de los servicios prestados.

El objetivo principal 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 ante los incidentes.

Los sistemas de información de **SYGRIS** deberán adaptarse a los cambios del entorno para garantizar la prestación continua de los servicios, así como estar protegidos frente a las amenazas con potencial para incidir en la disponibilidad, autenticidad, integridad, confidencialidad, trazabilidad, uso previsto y valor de la información y los servicios.

Se deberán implantar las medidas de seguridad exigidas por Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, (en adelante, ENS) 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.

La seguridad de la información deberá ser una parte integral del ciclo de vida de los sistemas de información desarrollados por **SYGRIS**, desde su diseño hasta su retirada, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y privacidad, así como las necesidades de formación y de financiación deberán ser identificados e incluidas en la planificación, en los servicios prestados por **SYGRIS** a las Administraciones Públicas.

Las áreas de negocio de **SYGRIS** deberán estar preparadas para prevenir, disuadir, detectar, reaccionar, conservar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

3. ALCANCE

Lo dispuesto por la presente Política es de aplicación a todos las soluciones y servicios de SYGRIS proporcionados a clientes, así como de obligado seguimiento por parte de todas las personas de SYGRIS, dentro del alcance siguiente:

“Sistema de gestión de seguridad de la información que da soporte a la gestión y prestación de los servicios de desarrollo, mantenimiento y soporte en producción de software.”

4. MARCO NORMATIVO

El Marco Regulatorio se encuentra recogido en el documento SYGRIS SGSI Registro Normativa.

Este documento se encuentra recogido en el Listado de documentación del SGSI y se gestiona de acuerdo con el Procedimiento de Gestión de la Documentación.

5. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Principio de confidencialidad: los sistemas de información deberán ser accesibles únicamente para aquellas personas usuarias, órganos y entidades o procesos expresamente autorizados para ello, con respeto a las obligaciones de secreto y sigilo profesional.

Principio de integridad y calidad: se deberá garantizar el mantenimiento de la integridad y calidad de la información, así como de los procesos de tratamiento de la misma, estableciéndose los mecanismos para asegurar que los procesos de creación, tratamiento, almacenamiento y distribución de la información contribuyen a preservar su exactitud y corrección.

Principio de disponibilidad y continuidad: se garantizará un alto nivel de disponibilidad en los sistemas de información y se dotarán de los planes y medidas necesarias para asegurar la continuidad de los servicios y la recuperación ante posibles contingencias graves.

Principio de gestión del riesgo: se deberá articular un proceso continuo de análisis y tratamiento de riesgos como mecanismo básico sobre el que debe descansar la gestión de la seguridad de los sistemas de información.

Principio de proporcionalidad en coste: la implantación de medidas que mitiguen los riesgos de seguridad de los sistemas de información deberá hacerse bajo un enfoque de proporcionalidad en los costes económicos y operativos.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

Principio de concienciación y formación: se articularán iniciativas que permitan a las personas usuarias conocer sus deberes y obligaciones en cuanto al tratamiento seguro de la información. De igual forma, se fomentará la formación específica en materia de seguridad de todas aquellas personas que gestionan y administran sistemas de información y telecomunicaciones.

Principio de prevención: se desarrollarán planes y líneas de trabajo específicas orientadas a prevenir fraudes, incumplimientos o incidentes relacionados con la seguridad.

Principio de mejora continua: se revisará el grado de eficacia de los controles de seguridad implantados, al objeto de adecuarlos a la constante evolución de los riesgos y del entorno tecnológico.

Principio de seguridad en el ciclo de vida de los sistemas de información: las especificaciones de seguridad se incluirán en todas las fases del ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Principio de función diferenciada: la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

Principio de vigilancia continua y reevaluación periódica. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

6. PREVENCIÓN

Se deberá evitar o prevenir que la información o los servicios se vean perjudicados por incidentes de seguridad.

Para ello, se ha de implantar salvaguardas mínimas de tipo organizativo y técnico contenidas en el ENS, así como cualquier control adicional identificado a través del análisis de riesgos.

Estos controles, junto con los roles y responsabilidades de seguridad, deberán estar claramente definidos y documentados.

Para garantizar el cumplimiento de la presente política, la Dirección de **SYGRIS** deberá:

- Autorizar los sistemas de información antes de entrar en operación

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

- Evaluar regularmente el estado de la seguridad de los sistemas de información, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica del estado de la seguridad de los sistemas de información por parte de terceros con el fin de obtener una evaluación independiente.

7. DETECCIÓN

Ante las consecuencias tan gravosas que podría provocar un incidente de seguridad, se deberá monitorizar las operaciones de forma continuada para así detectar anomalías en los niveles de prestación de los servicios y actuar de conformidad con lo establecido en el artículo 10 del ENS.

La monitorización es muy relevante cuando se establecen líneas de defensa de acuerdo con el artículo 9 del ENS.

En consecuencia, se deberán establecer los mecanismos de detección, análisis y reporte a los responsables regularmente y cuando se produzca una desviación significativa que se haya preestablecido como objetivo o normal.

8. RESPUESTA

Se deberá:

- a) Establecer los mecanismos para responder eficazmente a los incidentes de seguridad.
- b) Designar un punto de contacto (POC) para las comunicaciones con respecto a incidentes detectados internamente o en terceras partes.
- c) Establecer protocolos y procedimientos para el intercambio de información relacionada con el incidente.

Esto incluye las notificaciones antes las autoridades de control que sean competentes en la materia, tales como, la Agencia de Protección de Datos, en caso de que se vean afectados datos personales.

9. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios, se deberán desarrollar los planes de recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación del ENS, cuando ello sea exigible, como parte de su plan general de continuidad de negocio.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

10. PRINCIPIOS

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

- **Alcance estratégico:** La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un todo coherente y eficaz.
- **Responsabilidad proactiva:** Cumplir y demostrar el cumplimiento, para ellos se implementarán medidas proactivas encaminadas a garantizar el cumplimiento. Unido a lo anterior, se identificará, reportará y documentará a través de evidencias las acciones y medidas implementadas para alcanzar dicho cumplimiento, de forma que pueda demostrarse en todo momento.
- **Seguridad integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.
- **Gestión de Riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad. 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, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.
- **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
- **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
- **Seguridad y protección de datos desde el diseño y por defecto:** Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

11. REQUISITOS MÍNIMOS DE SEGURIDAD

La Política de Seguridad de la Información se establecerá de acuerdo con los principios básicos antes citados y se desarrollará aplicando los siguientes requisitos mínimos:

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
- h) Mínimo privilegio.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de actividad y detección de código dañino.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- o) Mejora continua del proceso de seguridad.

12. ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD

La seguridad deberá comprometer a todos los miembros de la organización.

La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II del ENS, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

- a) El responsable de la información determinará los requisitos de la información tratada
- b) El responsable del servicio determinará los requisitos de los servicios prestados.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

- c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
- d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.

En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo del Director General de SYGRIS, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

13. ANÁLISIS Y GESTIÓN DE LOS RIESGOS

Se realizará una gestión de riesgos de los sistemas de información desarrollados e implantados para el tratamiento de la información o la prestación de servicios.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II del ENS, se empleará una metodología reconocida internacionalmente.

Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

14. GESTIÓN DE PERSONAL

El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.

Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por el Director General de SYGRIS.

15. PROFESIONALIDAD

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

SYGRIS, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

SYGRIS determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo

16. AUTORIZACIÓN Y CONTROL DE LOS ACCESOS

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación del ENS deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

17. PROTECCIÓN DE LAS INFRAESTRUCTURAS E INSTALACIONES

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

18. ADQUISICIÓN DE PRODUCTOS Y CONTRATACIÓN DE SERVICIOS DE SEGURIDAD

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

- a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
- b) Otras certificaciones de seguridad adicionales que se requieran normativamente.
- c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

Para la contratación de servicios de seguridad se estará a lo señalado anteriormente y a lo dispuesto en el artículo 16 del ENS.

19. MÍNIMO PRIVILEGIO

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

- a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
- c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

20. INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

21. PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

22. PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión.

Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

23. REGISTRO DE ACTIVIDAD Y DETECCIÓN DE CÓDIGO DAÑINO

Con el propósito de satisfacer el objeto del ENS, 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 estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 del ENS podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá 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 una determinada actividad.

24. INCIDENTES DE SEGURIDAD

SYGRIS dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33 del ENS, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

25. CONTINUIDAD DE LA ACTIVIDAD

Los sistemas de **SYGRIS** dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

26. 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 la gestión de la seguridad de las tecnologías de la información.

27. CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS

Para dar cumplimiento a los requisitos mínimos establecidos en el ENS se adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:

- a) Los activos que constituyen los sistemas de información concernidos.
- b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
- c) Las decisiones que se adopten para gestionar los riesgos identificados.

Las medidas referidas tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados.

La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, del riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del ENS.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implantadas y las medidas del anexo II que compensan.

El conjunto será objeto de la aprobación formal por parte del Responsable de la seguridad.

28. ORGANIZACIÓN DE LA SEGURIDAD

La Política de Seguridad de **SYGRIS**, según detalla el Anexo II del ENS, en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la Organización.

La Dirección de **SYGRIS** es responsable de organizar las funciones y responsabilidades, la política de seguridad, así como de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

La estructura organizativa de seguridad, y jerarquía en el proceso de decisiones de **SYGRIS** la componen:

- Comité de Seguridad, la Dirección,
- Responsable de la Información,
- Responsable de Servicio,
- Responsable de Seguridad,
- Responsable del Sistema
- Delegado de Protección de Datos.

29. COMITÉ DE SEGURIDAD

El Comité de Seguridad de la Información de **SYGRIS** supervisa y coordina la seguridad de la información, reportando al Consejo de Administración, y está integrado por los responsables siguientes:

- Presidente: Director General
- Responsable de la información y del Servicio, que actuará además como secretario del Comité
- Responsable del Sistema de información, Vocal
- Responsable de Seguridad de la información, Vocal
- Delegado de protección de datos

El Comité de Seguridad tendrá las siguientes funciones:

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

1. Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información como marco de cumplimiento.
2. Elaborar la estrategia y posicionamiento en relación con la seguridad y privacidad de la información.
3. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad y privacidad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
4. Elaborar y revisar regularmente la Política para su aprobación por el Director General.
5. Aprobar la normativa de seguridad de la información.
6. Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
7. Supervisar y aceptar, en su caso, los riesgos residuales y recomendar posibles acciones de eliminación o mitigación.
8. Supervisar el desempeño de la gestión de incidentes de seguridad y emprender posibles actuaciones de mejora.
9. Promover las auditorías periódicas de seguridad que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.
10. Aprobar los planes de mejora de la seguridad y privacidad de la información.
11. Asignar y priorizar los recursos en materia de seguridad.
12. Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos tecnológicos desde su concepción inicial hasta su puesta en producción.
13. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
14. Informar regularmente del estado de la seguridad de la información al Director General

La Responsable de la información y del Servicio actuará como Secretario del Comité con las funciones:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

- Ejecutar directa o de forma delegada de las decisiones del Comité.

Corresponde a los vocales del Comité de Seguridad de la Información:

- a) Participar en las reuniones.
- b) Contribuir con ideas y sugerencias para el buen desarrollo de las reuniones.
- c) Todos miembros del Comité actuarán con voz y voto.

Corresponde al Delegado de Protección de Datos en el Comité asesorar en todos aquellos aspectos que afecten a la seguridad y privacidad de los datos personales:

- d) Participar en las reuniones.
- e) Emitir su parecer en aquellos aspectos relacionados con la seguridad de los datos personales, promover, en su caso, revisiones de análisis de riesgos, elaboración de evaluaciones de impacto en protección de datos, elaboración o modificación de procedimientos o políticas de seguridad de datos personales, entre otros.

El Comité se deberá reunir con carácter ordinario, al menos, una vez al año, y con carácter extraordinario cuando lo decida su Presidente.

El Comité quedará constituido cuando asista la mitad más uno de sus miembros y para que sus acuerdos sean válidos, deberán ser adoptados por mayoría simple de votos de las personas presentes. En caso de empate el voto de calidad lo tiene el Presidente, o en quien haya delegado.

El Comité podrá recabar del personal técnico la información o asesoramiento pertinente para el ejercicio de sus funciones. En caso necesario este personal podrá ser convocado por el Comité para su asistencia a las reuniones, en calidad de asesores, con voz, pero sin voto.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la seguridad y privacidad, prevalecerá la decisión adoptada por el Comité.

30. RESPONSABLE DE LA INFORMACIÓN

El Responsable de la Información conforme con los artículos 13 y 41 del ENS, establece las necesidades de seguridad de la información, determina los requisitos de seguridad de los servicios prestados y efectúan las valoraciones del impacto que tendría un incidente que afectara a su seguridad.

El Responsable de la Información tiene, además, en exclusiva, la potestad de modificar el nivel de seguridad requerido para la misma (Anexo II.5.7.2 del ENS)

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

asignando a cada información el nivel de seguridad requerido, siendo responsable de su documentación y aprobación formal.

Son funciones del Responsable de la Información, en resumen, dentro de su ámbito de actuación, las siguientes:

- Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información (artículo 41 del ENS).
- Determinar la categoría de los sistemas de información, según lo descrito en el Anexo I del ENS.
- Es, asimismo, responsable de aceptar los riesgos residuales calculados en el análisis de riesgos y de realizar su seguimiento y control.

Compatibilidades. Este rol únicamente podrá coincidir con la del Responsable de Servicio y el Responsable de Información en organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Sistema, aunque se trate de organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

31. RESPONSABLE DE SERVICIO

El Responsable del Servicio conforme con los artículos 13 y 41 del ENS, establece las necesidades de seguridad de los servicios prestados, determina los requisitos de seguridad de los servicios prestados y efectúan las valoraciones del impacto que tendría un incidente que afectara a su seguridad.

El Responsable del Servicio tiene, además, en exclusiva, la potestad de modificar el nivel de seguridad requerido para la misma (Anexo II.5.7.2 del ENS) asignando a cada información el nivel de seguridad requerido, siendo responsable de su documentación y aprobación formal

Son funciones del **Responsable del Servicio**, en resumen, dentro de su ámbito de actuación, las siguientes:

- Determinar los niveles de seguridad de los servicios proveidos, valorando los impactos de los incidentes que afecten a la seguridad de la información (artículo 41 del ENS).
- Determinar la categoría de los sistemas de información, según lo descrito en el Anexo I del ENS.
- Es, asimismo, responsable de aceptar los riesgos residuales calculados en el análisis de riesgos y de realizar su seguimiento y control.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

Compatibilidades. Es posible que coincidan en la misma persona u órgano las responsabilidades de la información y del servicio.

La diferenciación tiene sentido:

- Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
- Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.

Incompatibilidades.

- Este rol no podrá coincidir con el de Responsable de Seguridad, salvo en organizaciones de reducida dimensión que funcionen de forma autónoma.
- Este rol no podrá coincidir con el de Responsable de Sistema ni con el de Administrador de la Seguridad del Sistema, ni siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

32. RESPONSABLE DE SEGURIDAD

Conforme con el artículo 13 del ENS, es quien determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisa la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reporta sobre estas cuestiones.

Tiene como funciones:

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Gestionar la formación y concienciación en materia de seguridad.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

- h) Informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgos respecto de los márgenes aprobados.
- i) Da cuenta al Delegado de Protección de Datos sobre los aspectos que afecten a la seguridad de los datos personales.
- Violaciones de seguridad de los datos personales que afecten a la confidencialidad, disponibilidad e integridad de los datos personales.
 - Riesgos detectados y medidas correctoras oportunas relacionados con la seguridad de los tratamientos de datos personales.
 - Pedirá asesoramiento ante nuevas arquitecturas de seguridad, políticas y procedimientos que afecten al tratamiento de datos personales.

Incompatibilidades. No podrá coincidir con el Delegado de Protección de Datos.

33. RESPONSABLE DEL SISTEMA

El Responsable del Sistema de información y Responsable de operaciones, conforme con el artículo 13 del ENS, es quien se encarga de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

Serán funciones del Responsable del Sistema de Información, las siguientes:

- Desarrollar, operar y mantener los sistemas de Información durante todo su ciclo de vida, así como aprobar y/o ejecutar los cambios que afecten a la seguridad del modo de operación del sistema.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, siguiendo las indicaciones del Responsable de Seguridad.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Suspender el manejo de una determinada información o la prestación de un servicio si es informado de deficiencias graves de seguridad, previo acuerdo con el Responsable de dicha información o servicio, y con el Responsable de Seguridad.
- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad de los sistemas de información.
- La gestión de las autorizaciones concedidas a los usuarios las personas usuarias del sistema.
- La aplicación de los procedimientos de seguridad.
- Ejecutar los cambios de configuración del sistema de información.
- Asegurar el cumplimiento de los controles de seguridad y privacidad establecidos.
- Supervisar la instalación de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de Seguridad de la información de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

Compatibilidades. Podrá coincidir con el de Administrador de Seguridad del Sistema en organizaciones de una dimensión reducida o intermedia que tengan una estructura autónoma de funcionamiento.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Información, con el de Responsable de Servicio, ni con el de Responsable de Seguridad de la Información.

34. Delegado De Protección De Datos

Si bien SYGRIS no está obligada, ha nombrado a un Delegado de Protección de Datos encargado de asesorar y supervisar todos los aspectos relacionados con el tratamiento de datos de carácter personal, incluidos los aspectos de seguridad (integridad, confidencialidad y disponibilidad) y las brechas de seguridad de los datos personales. Su nombramiento se produce por otra vía ya que sus cometidos no se ciñen únicamente a aspectos de seguridad.

El Delegado de protección de datos desempeñará sus funciones, de acuerdo con lo dispuesto en el Artículo 39 del Reglamento General de Protección de Datos, prestando atención a los riesgos asociados a las operaciones de tratamiento.

Serán funciones del Delegado de protección de datos, las siguientes:

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

- Recabar información para determinar las actividades de tratamiento.
- Analizar y comprobar la conformidad de las actividades de tratamiento.
- Informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento.
- Recabar información para supervisar el registro de las operaciones de tratamiento.
- Asesorar en el principio de la protección de datos por diseño y por defecto.
- Asesorar sobre si se lleva a cabo o no las evaluaciones de impacto, metodología, salvaguardas a aplicar, etc.
- Priorizar actividades en base a los riesgos.
- Asesorar al Responsable de Tratamiento sobre el análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, en la evaluación de impacto en la protección de datos.
- Asesorar al Responsable de Tratamiento sobre áreas a cometer a auditorías, actividades de formación a realizar y operaciones de tratamiento a dedicar más tiempo y recursos.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Seguridad.

35. PROCEDIMIENTO DE DESIGNACIÓN

La Dirección General de SYGRIS designará formalmente, mediante comunicación por correo electrónico, a los responsables que siguen:

- Responsable de la Información y del Servicio.
- Responsable de la Seguridad.
- Responsable del Sistema.
- Delegado de Protección de Datos

36. RESOLUCIÓN DE CONFLICTOS.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad prevalecerá la decisión del Comité de Seguridad de la Información.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

37. DATOS DE CARÁCTER PERSONAL

SYGRIS, en calidad de Responsable o encargado de tratamiento, solo recogerá y tratará datos personales cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido.

A la vista de la aplicación del 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se deberán adoptar las medidas de índole técnica y organizativas necesarias, así como aquellas para dar cumplimiento a la normativa de protección de datos personales, tales como: el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y la designación del Delegado de Protección de Datos.

38. GESTIÓN DE LOS RIESGOS

Justificación

Todos los sistemas sujetos a esta Política deberán someterse a un **análisis de riesgos**, evaluando las amenazas y los niveles de riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar la aplicabilidad de las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el ENS, según lo previsto en el Artículo 7.

El análisis de los riesgos y su tratamiento deberá ser una actividad repetida regularmente, reevaluando y actualizando periódicamente las medidas de seguridad, para adecuar su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario, según lo establecido en el Artículo 10 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

- Cuando se reporten vulnerabilidades graves.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el Comité de Seguridad de la Información de **SYGRIS**.

Las fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del ENS y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional,

El análisis de riesgos contemplará los requisitos establecidos por el Artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 para decidir y establecer las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento.

Criterios de evaluación de riesgos

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes activos de información manejados y los diferentes servicios prestados.

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará **SYGRIS**, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de **SYGRIS** de forma grave.

Proceso de aceptación del riesgo residual

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información.

Los niveles de Riesgo residuales esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de esa Información.

Los niveles de Riesgo residuales esperados sobre cada Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por su Responsable de ese Servicio.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

39. OBLIGACIONES DEL PERSONAL

Todo el personal de **SYGRIS** tiene la obligación de conocer y cumplir con esta Política de Seguridad de la Información y la normativa de seguridad que la desarrolla, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los empleados de **SYGRIS** atenderán a una acción de concienciación en materia de seguridad de la información y protección de datos, al menos, una vez al año. Se establecerá un programa de formación y píldoras de concienciación, en particular a las nuevas incorporaciones, teniendo en cuenta siempre las disponibilidades presupuestarias.

Las personas con responsabilidad en el uso, tratamiento o administración de sistemas de información recibirán formación para el manejo seguro de los sistemas en la medida en la que los necesiten para acometer sus tareas laborales. La formación será obligatoria junto con la cualificación necesaria antes de asumir responsabilidades, tanto si es su primera asignación como si se trata de un cambio de puesto o de responsabilidades en el mismo.

40. TERCERAS PARTES

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

Asimismo, la Dirección de **SYGRIS** deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo del Director General (CEO), y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Cuando **SYGRIS** 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 atañe 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

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

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.

Del mismo modo, los terceros deberán designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de su Dirección, que canalizará y supervisión, tanto el cumplimiento de los requisitos de seguridad del servicio subcontratado que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio subcontratado.

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.

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de la presente Política, 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, asimismo, se les solicitará la aceptación de la presente Política, quedando sujeta a las obligaciones establecidas, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias y se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad y privacidad, 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, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos, sometiéndose a la aprobación de los responsables de la información y los servicios y del sistema de información.

Las terceras partes involucradas en tratamientos de datos de carácter personal deberán satisfacer los requisitos establecidos por SYGRIS y formalizar su relación como encargados de tratamientos.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

41. DESARROLLO Y ESTRUCTURA NORMATIVA

La estructura jerárquica de la documentación de seguridad de SYGRIS es la siguiente:

DOCUMENTO	DESCRIPCIÓN
Política	<p>Define las metas y expectativas de seguridad.</p> <p>Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos.</p> <p>Debe ser elaborada por el Comité de Seguridad y ser aprobada por la Dirección.</p>
Normativa	<p>Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema. Es de carácter obligatorio.</p> <p>Debe ser elaborada por personas expertas en la materia o por el Responsable de Seguridad y aprobada por el Comité de Seguridad.</p>
Procedimientos	<p>Determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución.</p> <p>Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar.</p> <p>Un procedimiento puede apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas.</p> <p>Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad.</p> <p>Debe ser elaborado por el Responsable del Sistema y aprobado por el Responsable de Seguridad</p>
Instrucciones técnicas	<p>Determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.).</p> <p>Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar.</p>

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

	<p>Una instrucción técnica debe ser clara y sencilla de interpretar.</p> <p>Debe documentar los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de la misma. A mayor nivel de detalle, mayor precisión y garantía de su correcta ejecución.</p> <p>Pueden ser elaborados por el Responsable del Sistema o Administrador del Sistema y deben ser aprobados por el Responsable de Seguridad.</p>
Guías o Buenas prácticas	<p>Las Guías del CCN son de obligado cumplimiento y ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.</p> <p>Las buenas prácticas, tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos.</p>

42. AUDITORÍA

El Sistema de Gestión de Seguridad y los sistemas de información de **SYGRIS** serán objeto, al menos, anualmente, de una auditoría regular ordinaria, interna y/o externa, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, asimismo, deberá auditarse siempre que se produzcan cambios o situaciones que puedan repercutir en el cumplimiento de las medidas de seguridad establecidas.

Los informes de auditoría se elevarán, para su aprobación, al Comité de Seguridad, decidiéndose las acciones a emprender, ya sean preventivas o correctivas.

43. REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por la Dirección General de **SYGRIS**, de acuerdo con el artículo 11 ENS.

Proyecto: SGSI	Versión: 1.0	Fecha:05/08/2024	
Política de seguridad de la información		Clasificación: Público	

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

Madrid, a 09 de agosto de 2024


Sergio Brihuega Moreno

Director General de CAMBRIDGE BUSINESS INITIATIVES SL