Política de Seguridad

Rev.	Fecha	Descripción	
3	29/09/2017	Adaptación al Esquema Nacional de Seguridad	
4	15/01/2021	Adaptación al art.11 del RD 951/2015 (ENS)	
5	22/07/2026	Revisión y actualización a nivel ALTO	
Preparado por		**Revisado por**	**Aprobado por**
Jorge Martín Martín **Fecha:** 22/07/2026		Javier Durán de Jesús **Fecha:** 22/07/2026	Javier Durán de Jesús **Fecha:** 22/07/2026

INDICE

1. Introducción **3**

2. Alcance **3**

3. Marco Normativo **3**

4. Principios de Seguridad **3**

4.1. Prevención 3
4.2. Respuesta 4
4.3. Recuperación 4
4.4. Líneas de defensa. 4
4.5. Reevaluación periódica. 5
4.6. Función diferenciada. 5

5. Requisitos mínimos **5**

5.1. Organización de la Seguridad y Responsabilidades 5
5.2. Gestión de riesgos 5
5.3. Obligaciones del personal 6
5.4. Profesionalidad 6
5.5. Autorización y control de los accesos 6
5.6. Protección de las instalaciones 6
5.7. Adquisición de productos 6
5.8. Seguridad por defecto 7
5.9. Integridad y actualización del sistema 7
5.10. Protección de la información almacenada y en tránsito 7
5.11. Prevención ante otros sistemas de información interconectados 8
5.12. Registros de actividad 8
5.13. Incidentes de seguridad 8
5.14. Continuidad de la actividad 8
5.15. Mejora continua del proceso de seguridad 8

6. Datos de Carácter Personal **8**

7. Desarrollo de la política de seguridad de la información **8**

8. TERCERAS PARTES 9

9. ANEXO I. DECLARACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 10

1. Introducción

Luce Innovative Technologies (en adelante, LUCE IT) depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, autenticidad, trazabilidad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Esto implica que deben aplicar las medidas de seguridad exigidas por la normativa de seguridad vigente, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y dar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

LUCE IT debe cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas y en los proyectos TIC.

LUCE IT debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo a la ISO 27001, Esquema Nacional de Seguridad y a la Normativa aplicable de Protección de Datos.

Esta Política de Seguridad sigue las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

2. Alcance

El Alcance de la presente política es la Gestión de Seguridad de la información asociada a los servicios de LUCE IT. El detalle se encuentra definido en el MG.01 Manual de Gestión.

3. Marco Normativo

Se cumplirá la legislación en materia de seguridad definida en el MG.01 Manual de Gestión y recogidas en el Registro de Legislación y Normativas

Las acciones que emprendamos en materia de seguridad de la información serán acordes con las mejores prácticas de seguridad, recogidas en las guías del CCN-STIC del Centro Criptológico Nacional y otras normas internacionalmente reconocidas.

4. Principios de Seguridad

4.1. Prevención

LUCE IT debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS y en la legislación de Protección de Datos, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

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

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

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

4.2. Respuesta

LUCE IT:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otras entidades.
- Establece protocolos para el intercambio de información relacionada con el incidente.

4.3. Recuperación

Para garantizar la disponibilidad de los servicios críticos, LUCE IT ha desarrollado planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

4.4. Líneas de defensa.

Nuestra estrategia de seguridad cuenta con líneas de defensa que nos permiten reaccionar adecuadamente a los incidentes que inevitablemente ocurran, ganando tiempo en la medida de lo posible, reduciendo la probabilidad de un fallo total y el impacto final del incidente.

4.5. Reevaluación periódica.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

4.6. Función diferenciada.

Hay distintas funciones que estarán diferenciadas para evitar conflictos de interés:

- En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.
- La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

5. Requisitos mínimos

5.1. Organización de la Seguridad y Responsabilidades

Las funciones y responsabilidades están definidas en el MG.01 Manual de Gestión, identificando las siguientes:

- Responsable del servicio
- Responsable de la información
- Responsable del Sistema
- Responsable de Seguridad
- Comité de Gestión

Los cargos serán nombrados por la Dirección a propuesta del Comité de Gestión, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

5.2. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año

- cuando cambie el tipo de información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Dirección establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Dirección dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de riesgos quedará documentada.

5.3. Obligaciones del personal

Según estipula el artículo 12 del Esquema Nacional de Seguridad, todos los miembros de LUCE IT tienen la obligación de conocer y cumplir esta política de seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Dirección disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de LUCE IT recibirán formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todos los empleados de LUCE IT, en particular a los de nueva incorporación.

5.4. 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.

El personal recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información en uso en la organización.

Los subcontratistas son cuidadosamente seleccionados y se les informa y forma para que presten sus servicios de acuerdo a nuestros niveles de profesionalidad y seguridad.

5.5. Autorización y control de los accesos

Los accesos a los sistemas de información están controlados y limitados a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

5.6. Protección de las instalaciones

Los sistemas se ubican en salas con acceso restringido. El acceso a las instalaciones también se encuentra restringido y controlado por medidas físicas.

5.7. Adquisición de productos

Cuando se presten servicios a clientes o se ceda información a terceros:

- Se les hará partícipes de la Política de Seguridad de la Información en el presente documento y de las normas de seguridad o procedimientos de seguridad relacionados con el servicio o la información afectados.
- Se establecerán canales de información y coordinación entre los respectivos responsables de gestión de la seguridad de la información y se establecerán procedimientos de seguridad para la reacción ante incidentes.

En los contratos de adquisición de sistemas o aplicaciones informáticas, de prestación de servicios tecnológicos, y también en el caso de contratos de prestación de servicios de otro tipo que implique el uso de servicios, aplicaciones o sistemas informáticos internos, se deberán tener en cuenta las medidas y consideraciones de seguridad de la información que resulten de aplicación, incluidas las de aplicación legal, en caso de acuerdos de cesión de sistemas, aplicaciones o acceso a servicios de terceros.

Siempre que sea posible y a juicio del Responsable de Seguridad se priorizará a aquellos proveedores que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

5.8. Seguridad por defecto

Los sistemas se han diseñado y configurado de forma que garanticen la seguridad por defecto:

- Los sistemas proporcionan la mínima funcionalidad que cada usuario necesita para la ejecución de sus tareas, asegurando que su uso sea sencillo y seguro.
- Las funciones de operación, administración y registro de actividad son las mínimas necesarias, y sólo son accesibles por personal autorizado y desde emplazamientos o equipos autorizados.
- En los sistemas en producción se eliminan o desactivan, mediante el control de la configuración, las funciones que no son de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

5.9. Integridad y actualización del sistema

La instalación de cualquier elemento físico o lógico sigue un procedimiento formal con distintos niveles de autorización hasta su puesta en producción.

Se hace un seguimiento riguroso del estado de seguridad de los sistemas y se atiende a las recomendaciones y especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que afecten a los elementos de los sistemas, para impedir o mitigar los riesgos que vayan apareciendo

5.10. Protección de la información almacenada y en tránsito

La propia naturaleza de nuestro negocio nos exige ser muy estrictos con la seguridad de la información almacenada en nuestros sistemas. Para ello se ha diseñado e implantado las medidas técnicas y organizativas que se recogen en nuestro Sistema de Gestión.

La protección de la información en tránsito también se considera crítica, por lo que se han implementado medidas apropiadas a nuestro tamaño y operativa para información en soportes físicos o lógicos, así como la transmitida por redes.

5.11. Prevención ante otros sistemas de información interconectados

El perímetro en el que se ubican nuestros sistemas se encuentra debidamente protegido, así como los puntos de interconexión con redes ajenas.

5.12. Registros de actividad

Con el fin de preservar la seguridad de nuestros sistemas, se recogen datos sobre la actividad de los usuarios con plenas garantías legales y de acuerdo con la normativa sobre protección de datos personales. Estos datos serán únicamente los necesarios para monitorizar, detectar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

5.13. Incidentes de seguridad

Nuestros sistemas de información cuentan con un sistema de detección y reacción frente a código dañino.

Estos y cualquier otro tipo de incidentes de seguridad se gestionan con las herramientas y procedimientos implantados al efecto, quedando registro de los mismos y de las actuaciones realizadas para resolverlos. Esta información se utiliza para evitar futuros incidentes, resolver antes lo que no se pueda evitar y tomar acciones de mejora.

5.14. Continuidad de la actividad

Los sistemas disponen de copias de seguridad y se han establecido los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

5.15. Mejora continua del proceso de seguridad

El proceso integral de seguridad implantado se actualiza y mejora en el marco de las normas que le aplican.

6. Datos de Carácter Personal

LUCE IT trata datos de carácter personal. El Documento de Seguridad recoge los sistemas de tratamiento afectados y los responsables correspondientes. Todos los sistemas de información de LUCE IT serán protegidos en base a los requisitos definidos en la normativa de Protección de Datos, así como con las medidas aplicadas para reducir los riesgos identificados. El Documento de Seguridad está ubicado en la Intranet de LUCE IT.

7. Desarrollo de la política de seguridad de la información

Esta Política se desarrollará por medio de la una Normativa de Seguridad que afronta aspectos específicos. La Normativa de Seguridad (**MG.01 Anexo II B Normativa de Seguridad**) estará a disposición de todos los miembros de la organización que necesiten conocerla en la Intranet de LUCE IT, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

8. Terceras partes

Cuando LUCE IT presta servicios se les hará partícipes a los clientes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando LUCE IT utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

9. Anexo I. Declaración de Política de Seguridad de la Información

El propósito de esta Política de la Seguridad de la Información es proteger los activos de información que intervienen en los servicios prestados por LUCE INNOVATIVE TECHNOLOGIES, en adelante LUCE IT. Es la política de LUCE IT asegurar que:

- La información está protegida contra pérdidas de disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad.
- La información está protegida contra accesos no autorizados.
- Su cumplen los requisitos legales aplicables.
- Se cumplen los requisitos del negocio y de las partes interesadas, respecto a la seguridad de la información y los sistemas de información.
- El Comité de Dirección valora los activos de información con los que cuenta LUCE IT 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 incidencias de seguridad son comunicadas y tratadas apropiadamente.
- Se establecen procedimientos para cumplir con la Política de Seguridad.
- Se evalúa el contexto interno y externo de la empresa y su impacto en la gestión de la seguridad de la información.
- La Dirección será la encargada 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.
- Cada empleado es responsable de cumplir esta Política y sus procedimientos según aplique a su puesto de trabajo.
- Es política de LUCE IT implementar, mantener y realizar un seguimiento del SGSI.

Esta política ha sido aprobada por el Comité de Dirección de LUCE IT y se revisará anualmente.