
	Manual de Gestión Anexo II Política de Seguridad	MG 01
		Página 1 de 8
		ED. 3


Política de Seguridad

Rev.	Fecha	Descripción
3	29/09/2017	Adaptación al Esquema Nacional de Seguridad
Preparado por		Revisado por
Jorge Martín Martín		Javier Durán de Jesús
		Aprobado por
		Javier Durán de Jesús
Fecha: 29/09/2017		Fecha: 29/09/2017
		Fecha: 29/09/2017

	<p style="text-align: center;">Manual de Gestión</p> <p style="text-align: center;">Anexo II Política de Seguridad</p>	MG 01
		Página 2 de 8
		ED. 3

1. Índice

1.	ÍNDICE	2
2.	INTRODUCCIÓN	3
3.	ALCANCE	3
4.	MARCO NORMATIVO	3
5.	RESPONSABILIDADES	3
6.	PRINCIPIOS DE SEGURIDAD	4
3.1	PREVENCIÓN	4
3.2	DETECCIÓN	4
3.3	RESPUESTA	4
3.4	RECUPERACIÓN	5
7.	DATOS DE CARÁCTER PERSONAL	5
8.	GESTIÓN DE RIESGOS	5
9.	DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	5
10.	OBLIGACIONES DEL PERSONAL	5
11.	TERCERAS PARTES	6
12.	ANEXO I. DECLARACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	7

	Manual de Gestión Anexo II Política de Seguridad	MG 01
		Página 3 de 8
		ED. 3

2. 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.

3. 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.


4. Marco Normativo

Se cumplirá la legislación en materia de seguridad definida en el MG.01 Manual de Gestión.

5. 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

	Manual de Gestión Anexo II Política de Seguridad	MG 01
		Página 4 de 8
		ED. 3

- 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.

6. Principios de Seguridad

3.1 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.

3.2 Detección


Dado que los servicios se puede 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.

3.3 Respuesta

LUCE IT:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.

	Manual de Gestión Anexo II Política de Seguridad	MG 01
		Página 5 de 8
		ED. 3

- 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.

3.4 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.

7. 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.

8. 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.

9. 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.

	<p style="text-align: center;">Manual de Gestión</p> <p style="text-align: center;">Anexo II Política de Seguridad</p>	MG 01
		Página 6 de 8
		ED. 3

10. 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.

11. 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 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 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.


	Manual de Gestión Anexo II Política de Seguridad	MG 01
		Página 7 de 8
		ED. 3

12. 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.

	Manual de Gestión Anexo II Política de Seguridad	MG 01
		Página 8 de 8
		ED. 3

Fecha

Firma