



Política de Seguridad de la Información

	Política de Seguridad de la Información	Versión
		1.4

PROPIEDADES DEL DOCUMENTO

Nombre del documento:	Política de Seguridad de la Información
Tipo de documento	Política
Clasificación documento	INTERNO
Resumen:	Este documento forma parte del cuerpo normativo de seguridad desarrollado para garantizar la correcta gestión y mantenimiento de la seguridad de la información, especificando las directrices y objetivos buscados, entre otros aspectos, que propicien un sistema de gestión efectivo y claro.
Propietario	Directora General

PARTICIPANTES (RELATIVOS A LA ÚLTIMA VERSIÓN DEL DOCUMENTO):

Elaborado por:	Responsable SGSI	Firmas / Acta
Revisado por:	Responsable Seguridad de la Información <i>Yamari Duarte Segovia</i>	Yamari Duarte Segovia 
Aprobado por:	Comité de Seguridad	09/09/2026

HISTORIAL DE REVISIONES

Versión	Fecha	Autor	Detalles de la versión
1.0	20/01/2024	Responsable de Seguridad de la Información	Versión Inicial del Documento
1.1	06/05/2024	Responsable SGSI (UST/Cyberproof	Se añade el rol de responsable de sistemas (Arquitectura y soporte)
1.2	27/05/2024	Responsable SGSI (UST/Cyberproof	Se añade el rol y responsabilidades del director de tecnología y del responsable de la información
1.3	06/05/2025	Responsable SGSI (UST/Cyberproof	Revisión transición a la ISO27K1:2022 y se añaden: los roles de RRHH, DPO, Legal. Se añaden los Objetivos del SGSI. Se revisa la sección Misión. Se incluye la metodología para la apreciación de riesgos. Corrección de erratas.
1.4	23/07/2026	OTS	Alineación con Guía 805 del CNN (POC). Funciones del DPD alineadas con Ilunion Grupo. Ampliación de las sedes del alcance, corrección de erratas

VIGENCIA

La aprobación y publicación de la versión 1.0 o posteriores de este documento expresa el respaldo de la Organización a su contenido. Las versiones anteriores que hayan podido distribuirse constituyen borradores o versiones obsoletas, por lo que su vigencia queda anulada por la última versión de este documento. En cualquier caso, todas las referencias documentales, con información referente a versiones, modificaciones, etc., aparecen descritas en esta ficha de versiones.

	Política de Seguridad de la Información	Versión
		1.4

En el caso de conflicto con otras normas o procedimientos de seguridad vigentes, será la opción más restrictiva la que prevalezca.

ÍNDICE

1. INTRODUCCIÓN	5
1.1 Ámbito de Aplicación	6
2. ALCANCE	6
2.1 Exclusiones del alcance	7
3. OBJETIVOS ESTRATÉGICOS	8
3.1 Objetivos Específicos del SGSI	9
4. MISION	11
5. PRINCIPIOS	12
5.1 Prevención	12
5.2 Detección	12
5.3 Respuesta	12
5.4 Recuperación	12
6. MARCO NORMATIVO	13
6.1 Otros documentos para consulta	14
6.2 Términos y Definiciones	14
6.3 Identificación, actualización y mantenimiento	14
7. ORGANIZACIÓN	15
7.1 Roles, funciones y responsabilidades en Seguridad de la Información	15
7.2 Dirección General	15
7.3 Comité de Seguridad de la Información	16
7.3.1 Responsable de Sistemas de la Información o CIO	18
7.3.2 Responsable de Seguridad de la Información o CISO	18
7.3.3 Responsables de Servicio (Contact Center y BPO)	21
7.3.4 Director de Tecnología (CTO)	21
7.3.5 Responsable de Seguridad Física	24
7.3.6 Director de Recursos Humanos	24
7.3.7 Delegado de Privacidad o DPO	25
7.3.8 Director del Área Legal	26
8. MEDIDAS DE PROTECCION	27
9. DATOS DE CARÁCTER PERSONAL	29
10. PROPIETARIO DEL RIESGO Y GESTIÓN DE RIESGOS	30
11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE DOCUMENTACIÓN	31

	Política de Seguridad de la Información	Versión
		1.4

12. OBLIGACIONES DEL PERSONAL	32
13. TERCERAS PARTES.....	33
14. REVISIÓN Y GESTIÓN DE EXCEPCIONES.....	34

1. INTRODUCCIÓN

Este documento tiene como misión dirigir y dar soporte a la gestión de la seguridad de la información de **ILUNION Contact Center BPO**, además de recoger formalmente los objetivos y establecer las estrategias para su consecución.

ILUNION Contact Center BPO considera la información un activo esencial para el cumplimiento adecuado de sus funciones y asume, por tanto, la responsabilidad de su protección. Es por ello por lo que depende en su práctica totalidad de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas son administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de la información tratada, o los servicios prestados.

Los sistemas TIC están protegidos contra las diferentes amenazas que se han considerado, incluidas las especificadas en el análisis de riesgos. Las medidas y salvaguardas que se han aplicado son aquellas recomendadas por diferentes estándares reconocidos. También se realiza un seguimiento continuo de los niveles de prestación de servicios, de las vulnerabilidades reportadas y se preparan respuestas efectivas a los incidentes identificados, de modo que se pueda garantizar la continuidad de los servicios prestados.

Todo **ILUNION Contact Center BPO** es consciente de que la seguridad TIC es una parte integral de todo el ciclo de vida del sistema y la información que maneja, desde su concepción hasta su retirada de servicio, pasando por decisiones como la adquisición de nuevos componentes o las actividades de explotación y, es por ello, por lo que todas las áreas de **ILUNION Contact Center BPO** están preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con los estándares reconocidos mencionados previamente.

La Dirección General, por medio de la presente política, declara su firme compromiso y apoyo al establecimiento de dicho Sistema de Gestión de Seguridad de la Información y a garantizar el cumplimiento de sus requisitos.

	Política de Seguridad de la Información	Versión
		1.4

1.1 Ámbito de Aplicación

Esta Política aplica a todo el personal de ILUNION Contact Center BPO, incluidos colaboradores externos, que están obligados a conocer, respetar y hacer cumplir dentro de su ámbito de responsabilidad, las medidas de seguridad establecidas para la protección de la información. Su incumplimiento manifiesto podrá acarrear el inicio de medidas disciplinarias y, en su caso, responsabilidades legales.

2. ALCANCE

Al determinar el alcance se ha tenido en consideración:

- Los factores externos e internos que afectan al SGSI de la organización.
- Los requisitos de las partes interesadas con relación a la seguridad de la información.
- Las interfaces y dependencias entre las actividades realizadas por la organización y las que se llevan a cabo por otras organizaciones.

El alcance del SGSI comprende:

Alcance	Detalle
Organizativo	ILUNION Contact Center BPO, que comprende las sociedades: • <i>ILUNION CEE C.CENTER, SA.</i> • <i>ILUNION CONT. CENTER, SA.</i>
Servicios/Procesos	• Servicios de Contact Center (CC). • Servicios de Gestión Documental (BPO).
Personal	Personal interno de ILUNION Contact Center BPO, así como personal de terceras partes.
Técnico	Sistemas de información e infraestructura de soporte y que son necesarios para la prestación de los servicios de negocio.
Sedes	A) CL JULIÁN CAMARILLO, 45. 28037 – MADRID. B) CL RUFINO GONZÁLEZ, 42-44. 28037 – MADRID. C) INDUSTRIAS 4 PLANTA 2 OFICINA 10. 28923 - ALCORCON (MADRID). D) PI CAN CALDERON, CTRA. SANTA CREU DE CALFELL, 105. 08830 - SANT BOI DE LLOBREGAT (BARCELONA). E) GRAN VIA DE LES CORTS CATALANES 184, 5º 4ª. 08038 – BARCELONA. F) AVDA. DE LA UNIVERSIDAD, S/N. PARQUE CIENTÍFICO TECNOLÓGICO. 10071 – CÁCERES. G) AV DE ELVAS, S/N, ED. PCTEX2 (CAMPUS UNIVERSITARIO). 06006 – BADAJOZ.

	Política de Seguridad de la Información	Versión
		1.4

Alcance	Detalle
	H) CALLE LOPEZ DEL VALLADO con CALLE MIGUEL INDURÁIN, 33002 OVIEDO – ASTURIAS. I) ISLA DE LA CARTUJA, CL LEONARDO DA VINCI, 13. 41092 – SEVILLA. J) AVD. REPÚBLICA ARGENTINA, 21B- PTA. 1ª. MÓDULO C-2. 41011 – SEVILLA.

2.1 Exclusiones del alcance

Quedan fuera de este alcance:

- Los sistemas de información y actividades que se llevan a cabo fuera de las sedes propias de ILUNION Contact Center BPO (servicios de Contact Center que se prestan desde las instalaciones de los clientes).
- Cualquier otra solución o servicio ofrecido por ILUNION Contact Center BPO diferente a los servicios descritos.
- ILUNION Emergencias: S.A.

	Política de Seguridad de la Información	Versión
		1.4

3. OBJETIVOS ESTRATÉGICOS

En esta política se definen los objetivos estratégicos de Seguridad de la Información y son:

- Considerar la información y los sistemas que la soportan como activos estratégicos, manifestando así su determinación en alcanzar los niveles de seguridad necesarios que garanticen su protección en cuanto a Autenticación, Confidencialidad, Integridad, Disponibilidad y Trazabilidad.
- Instaurar y mantener un Comité de Seguridad de la Información que gestione todas aquellas directrices que permitan preservar, resguardar y afianzar la seguridad de los activos de información y así mejorar la calidad de los servicios que se ofrecen a los clientes.
- Promover la implantación de los niveles de seguridad apropiados que permitan proteger los recursos de los sistemas de información y la información procesada, almacenada o transmitida por ellos. También deberán asegurar el cumplimiento de la legislación vigente en materia de protección de datos, velando por la confidencialidad, integridad y disponibilidad de la información. Se deberán asimismo gestionar los incidentes de seguridad que puedan afectar a la información o los sistemas que la soportan.
- Promover acciones de formación y concienciación en seguridad de la información dirigidas a todo el personal y garantizar la difusión de la presente Política de Seguridad de la Información, así como los documentos que la desarrollan.
- Crear y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) basado en estándares internacionales y códigos de buenas prácticas, para identificar, cuantificar, priorizar y tratar los riesgos, así como para evaluar y revisar el desarrollo de la Política de Seguridad de la Información como marco de definición de las directrices básicas de seguridad.
- Velar por la profesionalidad en materia de seguridad de la información, tanto del personal de ILUNION Contact Center BPO, de los proveedores y prestadores de servicio, como de los sistemas y procesos que soportan todo el marco de aplicación de esta política.
- Velar por la existencia de los mecanismos necesarios que aseguren la continuidad de las actividades críticas de ILUNION Contact Center BPO ante contingencias graves que afecten a los sistemas de información, permitiendo la recuperación de éstos en un periodo de tiempo aceptable.
- Promover la mejora continua en todos los aspectos relativos a seguridad de la información que garanticen que la aplicación de la presente política esté actualizada en el tiempo.

	Política de Seguridad de la Información	Versión
		1.4

3.1 Objetivos Específicos del SGSI

Ilunion Contact Center BPO, consciente de la importancia y sensibilidad de la información en su actividad, tiene como objetivo principal la implantación, gestión, revisión y mantenimiento (basado en la mejora continua) de un Sistema de Gestión de la Seguridad de la Información (SGSI) alineado con los requisitos de la norma UNE ISO/IEC 27001:2022 y el Esquema Nacional de Seguridad (2022) que asegure la:

- *Confidencialidad*: Proteger la información de accesos no autorizados.
- *Integridad*: Asegurar que la información es precisa y está completa.
- *Disponibilidad*: Garantizar que la información esté accesible cuando se necesita

Alienados con los objetivos estratégicos y el objetivo principal del SGSI, se establecen los siguientes objetivos específicos:

- 1) *Gestión de la apreciación del riesgo*: Identificar, evaluar y tratar los riesgos de seguridad de la información según el apetito de riesgo de Ilunion Contact Center BPO y las expectativas de nuestros clientes, empleados y socios comerciales.
- 2) *Marco de la política de seguridad de la información*: Desarrollar y hacer cumplir un conjunto de políticas, directrices y controles de seguridad de la información adaptados a las necesidades de Ilunion Contact Center BPO, basados en una evaluación de riesgos que cubra los aspectos organizativos, operacionales, técnicos y humanos de la empresa.
- 3) *Respuesta ante incidentes*: Desarrollar y mantener un plan de respuesta ante incidentes eficaz para minimizar el impacto de los incidentes de seguridad, brindando tranquilidad y confianza a nuestros clientes y empleados.
- 4) *Continuidad del negocio*: Establecer y probar planes de continuidad del negocio para asegurar que Ilunion Contact Center BPO pueda seguir operando de manera continua, incluso ante una interrupción significativa, garantizando la confianza de inversores, clientes y empleados.
- 5) *Cumplimiento legal y normativo*: Desarrollar e implementar medidas de seguridad que cumplan con los requisitos legales y normativos vigentes, asegurando el cumplimiento de Ilunion Contact Center BPO con las expectativas de las autoridades y organismos reguladores.
- 6) *Innovación y mejora continua*: Impulsar la mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI) para abordar el panorama de seguridad en constante evolución y satisfacer las expectativas de los clientes, empleados y otras partes interesadas, en términos de seguridad robusta.

	Política de Seguridad de la Información	Versión
		1.4

- 7) *Seguridad en la gestión de terceros:* Implementar controles que gestionen los riesgos asociados con terceros y garantizar que todos nuestros proveedores y colaboradores cumplan con los requisitos de seguridad de la información establecidos por Ilunion Contact Center BPO.
- 8) *Formación y concienciación en seguridad de la información:* Realizar capacitaciones periódicas sobre seguridad de la información para asegurar que todo el personal, tanto interno como externo, entienda sus roles y responsabilidades en la protección de la información, respondiendo a las necesidades de la empresa y del personal.

	Política de Seguridad de la Información	Versión
		1.4

4. MISIÓN

La misión de la Política de Seguridad es establecer las directrices, principios, requisitos y medidas que deben guiar a ILUNION Contact Center BPO, para garantizar la protección adecuada de la información y los servicios.

	Política de Seguridad de la Información	Versión
		1.4

5. PRINCIPIOS

5.1 Prevención

Los empleados de ILUNION Contact Center BPO, así como las personas encargadas de la seguridad de sus centros evitan, o al menos previenen en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, se han implementado las medidas mínimas de seguridad determinadas por el SGSI, así como cualquier control adicional identificado en el ya mencionado análisis de riesgos. Estos controles, además de los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados. Para garantizar el cumplimiento de esta política, los departamentos considerarán 3 apartados clave:

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

5.2 Detección

Dado que los servicios prestados se pueden degradar rápidamente debido a incidentes, desde una simple desaceleración hasta su detención, se monitoriza la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia. Se establecen mecanismos de detección, análisis y reporte que llegan a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

5.3 Respuesta

Todas las áreas de la organización establecen mecanismos para responder eficazmente a los incidentes de seguridad, designan puntos de contacto para las comunicaciones con respecto a incidentes detectados y establecen protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones con los Equipos de Respuesta a Emergencias (CERT).

5.4 Recuperación

Para garantizar la disponibilidad de los servicios, existe un Plan de continuidad de los sistemas TIC que forma parte íntegra de la gestión de seguridad de ILUNION Contact Center BPO.

	Política de Seguridad de la Información	Versión
		1.4

6. MARCO NORMATIVO

Las normas que se han tenido en cuenta a la hora de crear el marco normativo de ILUNION Contact Center BPO, configurar los sistemas informáticos y tratar datos de personas han sido:

- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.
- Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Estatuto de los Trabajadores (Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores).
- Convenio de Call center.
- Ley Igualdad de trato y oportunidades.
- Acuerdo Marco Europeo de Teletrabajo de 16 de Julio de 2002.
- Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.
Resolución de 20 de abril de 2023, de la Secretaría de Estado de Empleo y Economía Social, por la que se publica el Acuerdo del Consejo de Ministros de 14 de marzo de 2023, por el que se aprueba la Estrategia Española de Seguridad y Salud en el Trabajo 2023-2027.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Guía CCN-STIC 805, Esquema Nacional de Seguridad. Política de Seguridad de la Información.
- Guía CCN-STIC 801, Esquema Nacional de Seguridad. Responsabilidades y Funciones.

La evaluación de impacto normativo se especifica en el documento “NS13.RS00 - Legislación Aplicable”. La responsabilidad de la adecuación normativa es del Responsable de la Seguridad de la Información y Tecnología o un representante delegado por el mismo.

	Política de Seguridad de la Información	Versión
		1.4

6.1 Otros documentos para consulta

A continuación, se listan las diferentes normas y/o estándares de referencia indispensables para la aplicación de este documento. Para los documentos en los que no se especifique la fecha, aplicará la última edición de éste. Mientras que, para los documentos con fecha, aplicará únicamente la edición indicada.

- UNE-ISO/IEC 27001:2022: Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.
- ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Control de la seguridad de la información.
- UNE-ISO/IEC 27002: Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información.
- Catálogo de guías CCN-STIC del Centro Criptológico Nacional.

6.2 Términos y Definiciones

Para los fines de este documento, se aplican los términos y definiciones incluidos en:

- ISO/IEC 27000: Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.
- UNE-ISO/IEC GUIA 73:2009 IN.
- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo.

6.3 Identificación, actualización y mantenimiento

Todo el marco normativo del presente documento y los documentos asociados deberán ser revisados como mínimo anualmente y ante cualquier cambio de la legislación vigente que afecte a los sistemas de seguridad.

	Política de Seguridad de la Información	Versión
		1.4

7. ORGANIZACIÓN

Para gobernar la Seguridad de la Información de ILUNION Contact Center BPO se establece una estructura organizativa sólida y compacta, con roles claramente definidos y responsabilidades formalmente asignadas, que promuevan y garanticen el gobierno de la Seguridad de la Información en toda la organización.

7.1 Roles, funciones y responsabilidades en Seguridad de la Información

Se identifican, definen y asignan las responsabilidades de gestión, supervisión, ejecución y comunicación a las partes involucradas de todas las prácticas y procesos de seguridad. Por ello, se documentan las responsabilidades asociadas a los distintos procesos, siendo recomendable que se asocien a departamentos y no a roles, ya que esto facilita su mantenimiento ante cambios en las tareas de las personas.

Es necesario conocer y definir la relación de cada departamento de la organización con las actividades de seguridad de la información que hayan sido definidas. Del mismo modo, los miembros de estas áreas conocen lo que se espera de ellos en relación con la seguridad de la información. Es decir, sus compromisos y responsabilidades. Estas responsabilidades y compromisos son aceptados por las personas del departamento determinado que hayan sido designadas como responsables, quienes se deben comprometer a la ejecución de éstas.

Las personas a las que se les asignen responsabilidades de seguridad de la información podrán delegar estas actividades en otras personas. A pesar de ello, siguen siendo responsables de las tareas asignadas, debiendo asegurarse de la correcta ejecución de éstas, y rindiendo cuentas en relación con su estado.

7.2 Dirección General

El compromiso de la Dirección General de ILUNION Contact Center BPO es un elemento clave en el éxito de las iniciativas de seguridad, ya que tiene la responsabilidad máxima de la seguridad de la información en la Organización. Se encarga de dirigir, supervisar y tomar decisiones para gobernar la seguridad.

La Dirección General se compromete a implementar, mantener y mejorar la función de seguridad, por lo que su rol incluye como responsabilidades:

- Aprobar el alcance del SGSI.

	Política de Seguridad de la Información	Versión
		1.4

- Comunicar a la Organización la importancia de cumplir con los objetivos de las Políticas de alto nivel, sus responsabilidades legales y la necesidad de la mejora constante.
- Aprobar la Política de Seguridad.
- Designar a los diferentes roles encargados de realizar las tareas que requiere el sistema de gestión.
- Fijar y aprobar el apetito de riesgo.
- Aprobar y revisar los objetivos de seguridad. Alinearlos con los objetivos de negocio.
- Proporcionar los recursos necesarios para el aseguramiento del cumplimiento de estos objetivos y para la operación del Sistema de Gestión.
- Aprobar los planes de formación.
- Aprobar los planes de concienciación.
- Aprobar el Plan de Auditoría.
- Revisar los resultados de las auditorías para la toma de decisiones.
- Realizar una revisión del Sistema de Gestión (cumplimiento de objetivos...).
- Aprobar los planes de acciones correctivas.
- Aprobar los planes de mejora.
- Aprobar las políticas de seguridad.
- Aprobar el modelo de clasificación de la información.
- Aprobar el análisis de impacto.

7.3 Comité de Seguridad de la Información

El Comité de Seguridad de la Información se considera el primer órgano directamente responsable de las prácticas de seguridad definidas en el Cuerpo Normativo de Seguridad y dependiente de la Dirección General. Además, evalúa y aprueba cualquier cambio o medida que afecte de manera relevante al sistema de gestión de la seguridad, por lo que sus responsabilidades incluyen:

- Aprobar la estrategia de seguridad de la información.
- Fijar el umbral de riesgo aceptable, y aprobar el Plan de Tratamiento de Riesgos y el riesgo residual.
- Aprobar la Política de Seguridad de la Información y las Normas:
 - Establecer los objetivos de seguridad.
 - Alcance.
 - Roles y Responsabilidades.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.

	Política de Seguridad de la Información	Versión
		1.4

- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Revisar los planes de formación y concienciación.
- Revisar los planes de comunicación.
- Revisar el Plan de Auditoría.
- Revisar los resultados de las auditorías para la toma de decisiones.
- Revisar los planes de acciones correctivas.
- Revisar los planes de mejora.
- Revisar las políticas/normativas de seguridad.
- Revisar el modelo de clasificación de la información.
- Revisar el análisis de impacto.

Para evaluar el estado actual de la seguridad de la organización y ver cómo seguir mejorándolo de cara a futuro, se realizan reuniones con periodicidad al menos semestral (o menor si hay circunstancias extraordinarias), en las que, una vez concluidas, se realizan actas que registren varios aspectos de la reunión en cuestión: fecha, hora, asistentes, puntos tratados y, si aplica, siguientes pasos a tomar. Estas actas serán compartidas a modo informativo con la Dirección General.

Otras circunstancias que puedan acarrear reuniones extraordinarias del Comité de Seguridad son peticiones de alguno de sus componentes debido a cambios significativos en los servicios que se prestan, o incidentes de seguridad graves.

El Comité de Seguridad lo forman los siguientes cargos, con sus respectivos roles dentro del propio Comité:

- Dirección General Ilunion Contact Center BPO – **Copresidente.**
- Responsable de Seguridad de la Información – **Copresidente.**
- Dirección de Tecnología – **Vocal.**
- Dirección de Operaciones Contact Center (responsable de Servicio Contact Center) – **Vocal.**
- Dirección de Operaciones BPO (responsable de Servicio BPO) – **Vocal.**
- Dirección de Asuntos Generales y Compras (responsable de Seguridad Física) – **Vocal.**
- Dirección de Personas – **Vocal.**
- Dirección de transformación Digital – **Vocal.**
- Área GRC (responsable de Sistema de Gestión de Seguridad) – **Secretario.**

	Política de Seguridad de la Información	Versión
		1.4

De igual modo, si se considera necesario puede haber asistencia de personal no incluido en esta lista, si alguno de sus miembros fijos así lo considera.

Finalmente, las funciones de cada uno de los roles serán las siguientes:

- **Presidente:** Es su máximo representante y acuerda la convocatoria de las sesiones y fija el orden del día. Preside las sesiones, modela el debate. También tiene la potestad de invitar a personas relevantes en los aspectos a tratar del día (que actuarán como Vocales del Comité de Seguridad).
- **Vocales:** Asiste y participa en los debates y decisiones. Aporta datos e información para la adopción de acuerdos.
- **Secretario:** Convoca a los asistentes, dirige la reunión y levanta el acta.

Si bien las decisiones se adoptan por consenso o en su defecto, por el voto de la mayoría, en caso de empate el voto del presidente tiene doble valor.

7.3.1 Responsable de Sistemas de la Información o CIO

Designado por: Dirección General (el cargo de Responsable de la Información corresponde formalmente a la misma persona que el Director de Tecnología (ver: Director de Tecnología o CTO).

Funciones y responsabilidades:

- Desarrollar, operar y mantener el sistema.
- Definir la tipología y política de Gestión del Sistema.
- La conexión/desconexión de equipos/usuarios.
- Aprobar los cambios operativos que afecten al sistema.
- Implantar controlar e integrar medidas específicas de seguridad.
- La configuración autorizada y aprobación de modificaciones sustanciales del *hardware* y *software*.
- Determinar la Categoría del Sistema (proceso en Anexo I ENS) y las medidas de seguridad que deben aplicarse (Anexo II ENS).
- Elaborar y aprobar la documentación del sistema y determinar las responsabilidades de los involucrados en el mantenimiento, explotación, implantación y supervisión del sistema.
- Ha de investigar incidentes de seguridad y comunicarlo a quien corresponda.
- Establecer Planes de Contingencia o Emergencia y llevar a cabo ejercicios calendarizados.
- Aprobar el riesgo residual resultante en el servicio de la evaluación de riesgos.

7.3.2 Responsable de Seguridad de la Información o CISO

Designado por: Dirección General.

	Política de Seguridad de la Información	Versión
		1.4

Funciones: Proporcionar al órgano de gobierno de ILUNION Contact Center BPO apoyo y asesoramiento experto en materia de seguridad de la información y protección de activos; definir y supervisar los distintos elementos y campos que son necesarios para asegurar la correcta gestión de la seguridad de la información.

Responsabilidades:

- Elaborar los planes de seguridad de la información.
- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas.
- Establecer la metodología de apreciación del riesgo.
- Aprobar la Declaración de Aplicabilidad.
- Elaborar un Plan de Tratamiento del Riesgo.
- Difundir y poner a disposición de las partes interesadas la información sobre riesgos.
- Gestionar los recursos proporcionados para llevar a cabo los objetivos, estrategia y planificación de seguridad.
- Identificar necesidades de formación y concienciación. La capacitación será gestionada por el área encargada del plan de formación. El resto serán gestionadas diferentemente.
- Evaluar la eficacia de las acciones de formación y concienciación realizadas.
- Mantener registros de las competencias, acciones de formación y concienciación, etc., en materia de seguridad de la información.
- Revisar periódicamente el estado de la seguridad.
- Revisar los resultados de las auditorías y elevar las conclusiones al Comité de Seguridad.
- Mantener actualizados los indicadores de seguridad y presentarlos a la Dirección con la periodicidad que se establezca.
- Llevar un seguimiento sobre la resolución por parte de las áreas responsables de las no conformidades.
- Elaborar, aprobar, mantener y evaluar los procedimientos de seguridad.
- Realizar una coordinación de las medidas normativas, técnicas y organizativas de seguridad de la información.
- Desarrollar el documento de Organización de la seguridad de la información en el cual se recogerá quién asume cada una de las responsabilidades en seguridad, así como una descripción detallada de funciones y dependencias.
- Llevar la interlocución en materia de seguridad de la información con la Dirección General.
- Establecer los requisitos de seguridad que debe cumplir la instalación y el equipamiento utilizado en el teletrabajo.
- Definir los niveles de clasificación y medidas de protección de la información.

	Política de Seguridad de la Información	Versión
		1.4

- Establecer mecanismos de seguridad para evitar los accesos a datos o recursos no autorizados.
- Diseñar y mantener la arquitectura de seguridad.
- Definir y mantener la seguridad de la infraestructura.
- Supervisar que los procedimientos de restauración y recuperación de datos están definidos y se aplican correctamente.
- Supervisar que se apliquen medidas de seguridad durante el ciclo de vida de desarrollo seguro de aplicaciones.
- Gestionar los incidentes de SI.
- Realizar análisis forenses.
- Coordinar (o en su caso, asistir al responsable de continuidad) el Plan de continuidad de negocio y/o Recuperación de Desastres.
- Identificar los aspectos legales, contractuales y de negocio relativos a la seguridad de la información.
- Velar por el cumplimiento legal, coordinando las actuaciones necesarias con las unidades responsables.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.

El CISO podrá delegar estas funciones y responsabilidades en el Responsable del SGSI, y en este caso requiriendo estas, la aprobación del Responsable IT.

7.3.2.1 Responsable de Sistema de Gestión de Seguridad de la Información

Designado por: CISO, pudiendo delegar en la Dirección de Tecnología,

Funciones: Coordinar y mantener el sistema integrado de gestión.

Responsabilidades:

- Elaborar el alcance del SGSI.
- Elaborar y mantener la Política General de Seguridad.
- Identificar los riesgos y oportunidades de seguridad de la información.
- Gestionar los riesgos y las medidas implantadas para mantener éstos por debajo del umbral de riesgo establecido.
- Elaborar y mantener el procedimiento de gestión documental.
- Definir, gestionar y reportar la información de los indicadores.
- Realizar el reporte a las partes interesadas.
- Planificar y coordinar la ejecución de las auditorías internas.

	Política de Seguridad de la Información	Versión
		1.4

- Mantener actualizados los indicadores de seguridad y presentarlos a la Dirección con la periodicidad que se establezca.
- Llevar un seguimiento sobre la resolución por parte de las áreas responsables de las no conformidades.
- Gestionar y llevar un seguimiento de las no conformidades y acciones correctivas.
- Gestionar y llevar un seguimiento de las acciones de mejora.

7.3.3 Responsables de Servicio (Contact Center y BPO)

Designado por: Dirección General (como Dirección de Operaciones de Contact Center y BPO, respectivamente).

Función: Gestionar y controlar el servicio, garantizando los niveles de Calidad y Seguridad establecidos.

Responsabilidades:

- Determinar los requisitos (de seguridad) del servicio.
- Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios.
- Aprobar la categorización de los sistemas del servicio (ENS).
- Aprobar el riesgo residual resultante en el servicio de la evaluación de riesgos.

7.3.4 Director de Tecnología (CTO)

Designado por: Dirección General.

Función: Planificar, programar, gestionar y hacer seguimiento de los recursos tecnológicos de la empresa, garantizando especialmente que se dispone en cada momento de los medios que aseguran una prestación adecuada y eficiente de los servicios a sus clientes.

Responsabilidades:

- Diseñar, gestionar y controlar las plataformas tecnológicas e informáticas de cada centro de trabajo y de las externas, cuando así se acuerde con los clientes.
- Apoyar al Departamento Comercial durante la fase de análisis previo para la correcta elaboración de las propuestas.
- Extraer datos de los sistemas y elaborar los informes cuantitativos y cualitativos de las campañas.

	Política de Seguridad de la Información	Versión
		1.4

- Apoyar tecnológicamente al Departamento de Operaciones previo al inicio de las campañas y durante el desarrollo de las mismas.
- Seleccionar, adquirir y negociar con los proveedores de telefonía, sistemas e informática y con los profesionales que presten su colaboración a la empresa en estos campos.
- Realizar los proyectos de inversión aprobados en el Plan de Actuación de la compañía, respecto a las partidas de inversión de equipos informáticos y de telefonía.
- Gestionar los proyectos de desarrollo de nuevas soluciones, funcionalidades o mejoras para la operativa de Ilunion Contact Center BPO.
- Desarrollo e implementación de la estrategia tecnológica: Definir y ejecutar la estrategia tecnológica alineada con los objetivos de negocio de la empresa.
- Innovación y mejora continua: Identificar y promover la adopción de nuevas tecnologías que mejoren la eficiencia y competitividad de la empresa.
- Gestión del presupuesto tecnológico: Planificar y gestionar el presupuesto de TI, asegurando una asignación eficiente de recursos.
- Supervisión del equipo de TI: Liderar, gestionar y desarrollar al equipo de tecnología de la información, asegurando su alineación con los objetivos estratégicos de la empresa.
- Gestión de la infraestructura tecnológica: Supervisar la operación y el mantenimiento de la infraestructura tecnológica, asegurando su disponibilidad y rendimiento.
- Asegurar la integración de sistemas: Coordinar la integración de sistemas y aplicaciones para mejorar la eficiencia operativa.
- Planificación y gestión de proyectos tecnológicos: Dirigir y supervisar la implementación de proyectos tecnológicos, asegurando su entrega en tiempo y forma.
- Gestión de relaciones con *stakeholders*: Mantener relaciones efectivas con los *stakeholders* internos y externos, asegurando la alineación y colaboración en proyectos tecnológicos.
- Monitoreo de tendencias tecnológicas: Mantenerse actualizado sobre las tendencias tecnológicas emergentes y evaluar su aplicabilidad a la empresa.
- Asegurar el cumplimiento normativo: Garantizar que todas las soluciones tecnológicas cumplen con las normativas y regulaciones aplicables.

7.3.4.1 Responsables de Soporte y Arquitectura

Designado por: Director de Tecnología.

En Ilunion Contact Center BPO, la responsabilidad de los sistemas se divide en dos roles principales, Responsable de Soporte y Responsable de Arquitectura y Redes y sus funciones son:

4.3.4.1: Responsable de Soporte (CAU)

	Política de Seguridad de la Información	Versión
		1.4

Función: Definir y gestionar el mantenimiento de las infraestructuras tecnológicas de la compañía - equipamiento de puesto de usuario, equipamiento de comunicaciones (LAN, WAN) e infraestructuras de servidores.

Responsabilidades:

- Garantizar el cumplimiento de los niveles de servicio (SLA).
- Control y actualización de los *tickets*.
En colaboración con el resto del área, realizar seguimiento de los *tickets* de manera que permanezcan siempre actualizados.
- Apoyo y soporte al resto de técnicos del área.
- Documentar como se realiza la instalación y la configuración de los distintos aplicativos.
- Gestionar las redes networking: LAN, WAN.
- Dar soporte a las incidencias informáticas de los/as trabajadores/as.
- Funciones en Seguridad de la información:
 - Secretario y vocal en el Subcomité de Seguridad TIC.
 - Responsable de Sistemas de Información ILUNION Contact Center BPO en el área de Arquitectura y redes.
 - Propietario de los activos (servidores y *switches*).

4.3.3.2: Responsable de Arquitectura y redes

Función: Definición y mantenimiento de las redes informáticas internas y externas.

Responsabilidades:

- Dirigir y organizar el área de sistemas: Equipamiento de puestos de usuario, equipamiento de comunicaciones (LAN, WAN) e infraestructura de servidores.
- Implantar nuevos sistemas necesarios para la institución.
- Gestión con proveedores, documentación técnica y negociación con proveedores.
- Gestionar las redes Networking: LAN, WAN.
- Administración de *firewalls*: Gestionar los cortafuegos de los sistemas informáticos.
- Administrar los servidores bajo tecnología Windows y Linux.
- Funciones en Seguridad de la información:
 - Secretario y vocal en el Subcomité de Seguridad TIC.
 - Responsable de Sistemas de Información ILUNION Contact Center BPO en el área de Arquitectura y redes.
 - Propietario de los activos (servidores y *switches*).

	Política de Seguridad de la Información	Versión
		1.4

7.3.5 Responsable de Seguridad Física

Designado por: Dirección General (como Dirección de Asuntos Generales y Compras).

Funciones: Coordinar las medidas de seguridad física de las instalaciones.

Responsabilidades:

- Definir, implementar, gestionar y mantener las medidas de seguridad aplicables a la seguridad física de las instalaciones.
- Asegurar el cumplimiento de los controles de seguridad física.
- Informar al Responsable de Seguridad de la Información de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

7.3.6 Director de Recursos Humanos

Designado por: Dirección General.

Función: El área de RRHH adquiere diversos compromisos y funciones en relación con la seguridad de la información.

Responsabilidades:

- Verificación de las capacidades y referencias de los candidatos de un puesto de trabajo durante el proceso de selección.
- Requerimientos de seguridad de las Descripciones de Puestos de Trabajo (DPT's).
- Velar por la confidencialidad y privacidad en los términos y condiciones contractuales con los empleados.
- Velar por la difusión y comunicación de las políticas del SGSI.
- Gestionar los procesos sancionadores por violaciones de seguridad.
- Colaborar en los procedimientos seguros de alta/baja y modificación de los accesos de los empleados (físicos y lógicos).
- Colaborar en la concienciación y formación de los trabajadores, en materia de seguridad de la información.

	Política de Seguridad de la Información	Versión
		1.4

7.3.7 Delegado de Privacidad o DPD

El DPD, (o comité DPD) en el caso del Grupo, es una figura independiente que desempeña una función preventiva y responsable, supervisando y coordinando la política de protección de datos de Ilunion CC BPO. La responsabilidad del DPD abarca tanto el entorno interno de la empresa como sus relaciones externas, siendo el punto de conexión entre el responsable del tratamiento, el interesado y las Autoridades de Control.

Designado por: Dirección General.

La designación de un DPD no exime al Grupo de su responsabilidad por las diversas actividades de tratamiento realizadas con datos personales o de cumplir con las disposiciones del Reglamento.

Función: Supervisar el cumplimiento de lo dispuesto en el RGPD y la LOPD-GDD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

En este sentido, recaen dentro de la organización determinadas obligaciones en relación a la actividad de la figura del DPD, con el fin de que este pueda desarrollar libremente su cometido.

Se presentan a continuación las funciones mínimas a desarrollar por el DPD, de acuerdo con los artículos 38 y 39 del RGPD:

Funciones mínimas:

- Punto de contacto con la Autoridad de Control y con los Interesados
- Cooperación con la Autoridad de Control y Realización de las Consultas Previas ante la Autoridad de Control.
- Asesoramiento en materia de protección de datos.
- Control y supervisión. Deberá supervisar el cumplimiento:
 - De la normativa comunitaria y nacional en materia de protección de datos
 - De las políticas del Responsable o del Encargado del tratamiento en materia de protección de datos personales, la asignación de responsabilidades, y las auditorías correspondientes.
- Formación: Deberá promover la concienciación y garantizar la formación del personal que trata datos de carácter personal con el fin de informarles de sus derechos.
- Asesoramiento de los PIAs
- Supervisar y mantener el Registro de tratamientos.
- Comunicación de las Brechas de Seguridad a la Autoridad de Control e interesados cuando proceda.

	Política de Seguridad de la Información	Versión
		1.4

- Evaluar y asegurar relaciones con terceras partes en el cumplimiento del RGPD.
- Ser el punto de contacto y gestionar el ejercicio de los derechos de los interesados

El modelo de gobierno, las funciones detalladas, obligaciones y otros aspectos del modelo de gobierno para la protección de datos se describe en el documento corporativo:

- *PS.05.02 - Modelo de Gobierno RGPD y DPD.pdf*

7.3.8 Director del Área Legal

Designado por: Dirección General.

Función: Planificar, programar, gestionar y hacer seguimiento de los recursos tecnológicos de la empresa, garantizando especialmente que se dispone en cada momento de los medios que aseguren una prestación adecuada y eficiente de los servicios a sus clientes.

Responsabilidades:

- Asegurar que se identifiquen todas las leyes, regulaciones, normativas, y obligaciones contractuales aplicables a la seguridad de la información.
- Informar al SGSI en cuanto a cambios en las leyes que puedan impactar las operaciones de seguridad de la organización.
- Supervisar los requisitos legales y contractuales, especialmente en temas como protección de datos personales (por ejemplo, GDPR si aplica), confidencialidad e integridad de la información.
- Participar y revisar los acuerdos establecidos con proveedores y terceros, y los contratos, para garantizar que cumplen con los estándares de seguridad de la información.
- Colaborar con el equipo del SGSI para evaluar riesgos relacionados con el cumplimiento de normativas y regulaciones.
- Colaborar en la capacitación del personal sobre las implicaciones legales del manejo de información y las consecuencias del incumplimiento.

	Política de Seguridad de la Información	Versión
		1.4

8. MEDIDAS DE PROTECCION

Con el fin de garantizar la seguridad de los sistemas de información de Ilunion Contact Center BPO, se establecen medidas de protección mínimas que se exigirán en proporción a los riesgos identificados en cada sistema y que pueden variar en el tiempo.

- **Autorización y control de los accesos.**

Ilunion Contact Center deberá contar con políticas claras de acceso y control de acceso, para garantizar que la información solo sea accesible por el personal autorizado y que se mantengan los permisos adecuados. Ilunion Contact Center BPO establece los controles para la autorización y control de accesos en la norma “NS09- Norma de Control de Acceso Lógico”.

- **Protección de las instalaciones.**

Ilunion Contact Center BPO deberá establecer controles de seguridad para prevenir los accesos físicos no autorizados, los daños y las intromisiones en las instalaciones, los equipos y la información de la Organización. (ver: “NS04 - Norma de Seguridad Física”).

- **Adquisición de productos de seguridad y contratación de servicios de seguridad.**

Como norma general, Ilunion Contact Center BPO adquirirá todos los productos y servicios que afecten la seguridad de la información según la normativa establecida. Ilunion Contact Center BPO establece los controles para la adquisición de productos de seguridad y la contratación de servicios en su norma “NS14 - Norma de Adquisición, Desarrollo y Mantenimiento”.

- **Mínimo privilegio.**

Los sistemas de Ilunion Contact Center BPO deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto, respetando el principio de mínimo privilegio. Es decir, otorgando a los usuarios y procesos únicamente los permisos y accesos necesarios para realizar sus funciones específicas, sin proporcionar privilegios adicionales que puedan comprometer la seguridad del sistema.

- **Protección de la información almacenada y en tránsito.**

Ilunion Contact Center BPO deberá implementar técnicas de encriptación de datos, tanto en tránsito, como en reposo, con el fin de proteger la información. (ver: NS05 - Norma de Controles Criptográficos).

- **Prevención ante otros sistemas de información interconectados.**

	Política de Seguridad de la Información	Versión
		1.4

Al conectar redes internas y/o externas, el/la responsable de red debe hacerlo siempre ajustándose a las condiciones de conexión de ambas redes y debe instalar mecanismos de identificación, autenticación, control de acceso, etc., en función del tipo de información manejada, los sistemas que estén conectados y los nuevos riesgos que se originen por interconectar las redes.

La conexión de una red interna con una externa:

- Nunca será directa, sino que se interpondrá una DMZ entre ambas en la que no se podrá realizar proceso de datos de negocio y los recursos de almacenamiento deberán ser temporales.
- Se debe implementar una separación lógica entre la red interna y la DMZ externa, y medidas de seguridad para evitar el acceso no autorizado desde el exterior.

- **Registro de la actividad y detección de código dañino.**

Ilunion Contact Center BPO realizará tareas de monitorización y detección de sus sistemas con el fin de detectar posibles incidentes que afecten al sistema de información, mediante un servicio de monitorización (SOC). Además, se definen las medidas de protección de las comunicaciones y la arquitectura en la norma *NS15 - Norma de Seguridad en las Telecomunicaciones*.

- **Incidentes de seguridad.**

Cualquier/a profesional de Ilunion Contact Center BPO o colaborador externo que detecte la existencia de un incidente de seguridad o tenga indicios de que pudiera producirse, deberá notificarlo lo antes posible al responsable de seguridad de la información, quien escalará hasta su resolución siguiendo el procedimiento corporativo detallado en la Norma de Gestión Incidentes de Seguridad de la Información.

En el transcurso de la atención de la incidencia, el/la responsable al que se escale su resolución deberá contactar con las áreas y personas afectadas y tomar las acciones pertinentes para minimizar daños y evitar la pérdida de evidencias o información valiosa.

- Se debe evitar el borrado de ficheros y la destrucción de material o documentos hasta que se dé por cerrada la incidencia.
- Se debe procurar mantener la cadena de custodia de cualquier elemento que pueda ser utilizado como evidencia en caso de que la incidencia derive en acciones legales.
- En la medida de lo posible, cualquier investigación o análisis del incidente se realizará sobre copias de los soportes de información originales.

Tras la resolución de un incidente grave, si el Comité de Seguridad lo considera oportuno, se podrán iniciar las acciones legales o disciplinarias oportunas.

	Política de Seguridad de la Información	Versión
		1.4

9. DATOS DE CARÁCTER PERSONAL

ILUNION Contact Center BPO trata datos de carácter personal. Todos los sistemas de información del ILUNION Contact Center BPO se ajustarán a los niveles de seguridad requeridos por la normativa mencionada en el presente documento para la naturaleza y finalidad de los datos de carácter personal recogidos, entre los que se incluyen, por ejemplo, la realización y actualización de Registro de Actividades de Tratamiento (RAT) y Evaluaciones de Impacto de Protección de Datos (EIPD).

Grupo ILUNION tiene un DPO (dpd@ilunion.com). Paralelamente ILUNION Contact Center BPO, cuenta con un Delegado de Protección de Datos para la entidad como responsable de todos los datos de carácter personal y su correcto manejo.

El Responsable de la Seguridad de la Información, actúa como DPD. Cuando Ilunion CC BPO actúe como encargado del tratamiento o contrate con prestadores, incluyendo los relacionados con el uso de la nube, el DPD será el Punto de Contacto o POC.

	Política de Seguridad de la Información	Versión
		1.4

10. PROPIETARIO DEL RIESGO Y GESTIÓN DE RIESGOS

El propietario del riesgo es la persona que tiene la responsabilidad y la autoridad para gestionar un riesgo (no tiene por qué ser la persona que ejecuta los controles).

La gestión de la apreciación del riesgo se realiza siguiendo una aproximación metódica, con el fin de garantizar que los datos obtenidos resulten fiables, comparables y reproducibles y cumple con los siguientes requisitos:

- *Metódica*: No es improvisada.
- *Objetiva*: El método utilizado es objetivo y no depende de la arbitrariedad.
- *Repetible*: Permite conseguir resultados repetibles en el tiempo.
- *Documentada*: Toda modificación, concreción o criterio adoptado en la aplicación de dicha metodología ha sido documentado, al objeto de que cualquier persona autorizada pueda consultarla y continuarla.

Periódicamente los activos de la información sujetos a esta política han sido sometidos a una evaluación de riesgos, siguiendo la metodología establecida, de modo que se han podido tomar las medidas de seguridad pertinentes y se obtiene un riesgo residual que está por debajo del umbral de riesgo que la organización ha establecido como aceptable.

Con la finalidad de tomar medidas complementarias o modificar las ya existentes, esta evaluación se repetirá:

- Regularmente, y como mínimo una vez al año;
- cuando haya cambios relevantes en la infraestructura IT;
- cuando cambie la información manejada;
- cuando cambien los servicios prestados;
- cuando ocurra un incidente grave de seguridad; y
- cuando se reporten vulnerabilidades graves que comporten modificar el actual análisis.

	Política de Seguridad de la Información	Versión
		1.4

11. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE DOCUMENTACIÓN

Esta Política de Seguridad de ILUNION Contact Center BPO complementa a la Política de Seguridad corporativa del Grupo ILUNION y la Fundación ONCE.

El responsable de los activos de información será el Responsable del Servicio asociado al activo de ILUNION Contact Center BPO que maneje esa información. Dicho responsable tiene en exclusiva la potestad de modificar el nivel de seguridad requerido en cada momento para la información.

La clasificación de la información utilizada por los empleados de ILUNION Contact Center BPO está definida en el documento **NS08.PS02 - Clasificación y Protección de la Información** atendiendo a los siguientes niveles de clasificación: Pública, Interna, Restringida y Confidencial. Esta clasificación de la información se basa en su confidencialidad, disponibilidad, integridad, autenticidad y trazabilidad.

Es responsabilidad del propietario de la información asegurar que las medidas de seguridad implantadas para proteger dicha información son acordes a los niveles de clasificación y es responsabilidad de todos los trabajadores de la organización, cumplir con las medidas de seguridad establecidas para cada nivel. Debe existir un registro del histórico de los cambios, así como la fecha y responsable del cambio.

La estructura, la gestión documental y el contenido de ésta, acorde al tipo de documentación, se define en el documento:

- **MN01 - Marco Normativo SGSI**

Las directrices para su protección y acceso se definen en:

- **MS01.PS01 - Procedimiento de Control y Gestión Documental del SGSI**

	Política de Seguridad de la Información	Versión
		1.4

12. OBLIGACIONES DEL PERSONAL

Todos los miembros de ILUNION Contact Center BPO tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros del ILUNION Contact Center BPO estarán sujetos a actividades de concienciación en materia de seguridad TIC al menos, una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación, como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

	Política de Seguridad de la Información	Versión
		1.4

13. TERCERAS PARTES

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

Cuando se utilicen servicios de terceros o se 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 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.

	Política de Seguridad de la Información	Versión
		1.4

14. REVISIÓN Y GESTIÓN DE EXCEPCIONES

Toda la documentación del Marco Normativo se revisa y actualiza anualmente o cuando se producen cambios significativos. La revisión de la documentación se planificará en función de su antigüedad, grado de obsolescencia, acciones correctivas en curso y observaciones recibidas.

En cualquiera de los casos, la derogación de un documento se comunicará al responsable de Seguridad de la Información y al responsable del Sistema de Gestión de Seguridad de la Información a efectos de que éstos mantengan actualizado el repositorio de documentación.

Toda excepción al presente documento es registrada e informada en el Comité de Seguridad. Asimismo, cualquier violación de ésta puede resultar en la toma de las acciones disciplinarias correspondientes. Es responsabilidad de todos los miembros de la organización notificar cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas en el presente documento.