LEGALITAS.COM

USO PÚBLICO

Política de Seguridad de la Información y Continuidad de Negocio

POL[A.17]-01

	Elaborado	Revisado	Aprobado	
Nombre	LEGALITAS	Responsable SGI	Comité SGI	Consejo Administración
Cargo	Responsable SGI	Responsable SGI	Comité SGI	Consejo Administración
Fecha	27/07/2018	03/09/2018	03/09/2018	19/06/2020

SÍNTESIS DEL DOCUMENTO	
Ámbito de difusión:	Uso Público
Consultar en caso de duda:	Responsable de SGI

CONTROL DE CAMBIOS					
Edición		Autor	Resumen de modificaciones	Revisado	Aprobado
Nº	Fecha				
1.0	18/09/2014	LEGALITAS	Primera versión del documento	Comité SGCN-SGSI	Comité SGCN-SGSI
2.0	26/01/2016	LEGALITAS	Actualización del documental	Comité SGCN-SGSI	Comité SGCN-SGSI
3.0	27/02/2017	LEGALITAS	Revisión y actualización del documento	Comité SGCN-SGSI	Comité SGCN-SGSI
4.0	26/12/2017	LEGALITAS	Integración Política SGSI y SGCN	CSGI	CSGI
5.0	12/03/2018	LEGALITAS	Revisión y actualización del documento	CSGI	CSGI
6.0	27/07/2018	LEGALITAS	Actualización del documento. Cambio de nomenclatura.	CSGI	CSGI / Consejo de Administración
7.0	15/06/2020	LEGALITAS	Revisión sin cambios.	CSGI	CSGI / Consejo de Administración

Índice

1. DECLARACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE NEGOCIO

El presente documento tiene por objeto establecer la política de seguridad de la información y continuidad de negocio para **LEGÁLITAS** en base a los requisitos dispuestos en los estándares de seguridad de la información ISO/IEC 27001:2013 e ISO/IEC 22301:2012, asegurando así la confidencialidad, integridad y disponibilidad de los sistemas de información de **LEGÁLITAS** y por supuesto, garantizando el cumplimiento de todas las obligaciones legales aplicables.

Como punto fundamental de la presente política está el soporte a la implantación, operación, mantenimiento y mejora continua de un Sistema de Gestión Integrado que proporcione la base de trabajo para la integración de sendos sistemas, basados en la Gestión de la Seguridad de la Información según la norma ISO/IEC 27001:2013 y en la Gestión de la Continuidad de Negocio, según lo establecido en la norma ISO/IEC 22301:2012.

2. POLÍTICA DE SEGURIDAD Y CONTINUIDAD.

2.1. Principios.

La política de seguridad y continuidad de **LEGÁLITAS** tiene por objetivo marcar las pautas de alto nivel a seguir para que todos los tratamientos de información relativos a los procesos de negocio indicados en el alcance se realicen de forma segura y únicamente por personal autorizado, así como proteger la información y los procesos asociados de la organización preservando los siguientes principios:

- **Confidencialidad de la información**: garantizar que la información sea accesible sólo para quien esté autorizado a tener acceso a la misma.
- **Integridad de la información**: garantizar la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad de la información**: garantizar que sólo los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
- **Establecer** como máxima prioridad **la protección de todo el personal** teniendo en cuenta tanto situaciones de normalidad como de contingencia.

- **Garantizar la correcta implantación**, operación, evaluación y mantenimiento del Sistema de Gestión de Continuidad del Negocio y de Gestión de la Seguridad de la Información, en aras de obtener una mejora continua de los mismos.
- **Establecer controles** sobre todas las partes críticas para el servicio prestado por **LEGÁLITAS** asegurar la información y la continuidad de sus actividades.
- **Garantizar** que las **medidas de seguridad de la información**, los procesos y los planes de continuidad de Negocio se implantan, desarrollan y mejoran de forma continua, haciendo partícipes a todos los departamentos según su nivel de involucración.
- **Garantizar** que **los procesos críticos** se recuperan dentro de los márgenes de tiempo requeridos por los planes de continuidad del negocio y se lleven a cabo preservando la Integridad, Confidencialidad y Disponibilidad de la información asociada.
- **Asegurar el adecuado funcionamiento** de los planes de contingencia a través de la realización de pruebas que permitan comprobar la eficiencia de las acciones de recuperación establecidas.
- **Garantizar que todo el personal permanece informado** de las responsabilidades asociadas a su cargo en relación a la Continuidad del Negocio y Seguridad de la Información.
- **Proveer canales de comunicación** con los distintos grupos de interés y partes interesadas para conocer sus expectativas y necesidades, al tiempo que **LEGÁLITAS** comunica sus compromisos, respecto a la seguridad de la información y continuidad de negocio.
- **Definir Comités y equipos** de Continuidad de Negocio y Seguridad de la Información formados por personal con la preparación y experiencia adecuada, para asegurar una adecuada coordinación y participación en la toma de decisiones enfocadas a la protección de la información y la continuidad de negocio de la Organización.
- **Garantizar el cumplimiento con lo establecido en el cuerpo documental** del Sistema de Gestión Integrado (SGI), respecto a la Gestión de la Seguridad de la Información y la Gestión de la Continuidad de Negocio.
- **Garantizar el cumplimiento de la legislación vigente** y de los compromisos contractuales adquiridos.
- Garantizar el cumplimiento de la normativa en materia de protección de datos y la correcta adecuación de los procesos de la empresa a la misma.

Estos principios básicos se deben preservar y asegurar en cualquiera de las formas que adopte la información, ya sea en formato electrónico, impreso, visual o hablado, e independientemente de que sea tratada en las dependencias de **LEGÁLITAS** o fuera de ellas y quedar reflejadas en los planes de contingencia que se elaboren para asegurar la resilencia de la Compañía.

Asimismo, estos principios se deberán contemplar en las siguientes áreas de seguridad y continuidad:

- **Física**: Comprendiendo la seguridad de las dependencias, instalaciones, sistemas hardware, soportes y cualquier activo de naturaleza física que trate o pueda tratar información y que sea necesario para asegurar la continuidad de la actividades de negocio de la Compañía en caso de contingencia.
- **Lógica**: Incluyendo los aspectos de protección de aplicaciones, redes y prototipos de comunicación electrónica y sistemas informáticos, así como su reflejo en los planes de continuidad de negocio.
- **Político-corporativa**: Formada por los aspectos de seguridad y continuidad de negocio relativos a la propia Compañía, a las normas internas, regulaciones y normativa legal.

Teniendo en cuenta los principios básicos anteriormente citados, se han definido objetivos específicos de seguridad y continuidad de negocio, siguiendo la regla S.M.A.R.T, para que los mismos sean:

- **Específicos** (Specific): Suficientemente claros, precisos y determinados.
- **Medibles** (Measurable): Permitiendo que pueda cuantificarse su consecución.
- **Alcanzables** (Achievable): Factibles, teniendo en cuenta los recursos.
- **Realistas** (Realistic): Ajustados a la realidad del entorno y los recursos.
- **Limitados en el tiempo** (Time bound): Definiendo un periodo de realización para cada uno de ellos.

2.2. Objetivos.

Los objetivos de Seguridad de la Información y Continuidad de Negocio que se persiguen desde **LEGALITAS** son:

- **O1: Salvaguardar** los activos de la Organización dentro del alcance mediante la implantación de controles y salvaguardas, lo que permitirá reducir el impacto o la

probabilidad de ocurrencia de las amenazas que pudieran materializarse sobre los mismos a la vez que se reduce su efecto sobre la actividad de la compañía.

- **O2: Mitigar** los efectos adversos de los incidentes de seguridad.
- **O3: Establecer** mecanismos de clasificación de la información que permitan proteger adecuadamente cada activo en base a su criticidad y su inclusión en los planes de continuidad.
- **O4: Definir los roles y responsabilidades** en materia de seguridad y continuidad necesarias para garantizar la correcta gestión del SGI.
- **O5: Elaborar** un cuerpo documental adscrito a la presente Política que garantice el correcto gobierno del SGI.
- **O6: Definir** claramente las acciones asociadas a los incumplimientos de la Política de Seguridad.
- **O7: Evaluar los riesgos** a los que se ven sometidos los activos dentro del alcance, lo que debe permitir la correcta definición y aplicación de controles y salvaguardas para protegerlos, así como su necesidad para asegurar la continuidad de la actividad de la Compañía en circunstancias de contingencia.
- **O8: Verificar el correcto funcionamiento** de las salvaguardas, controles y planes de contingencia mediante la realización de auditorías internas independientes.
- **O9: Llevar a cabo programas de formación** que eduquen y conciencien a los empleados en materia de Seguridad de la Información y Continuidad de Negocio así como en materia de protección de datos.
- **O10: Evaluar y hacer cumplir la legislación** vigente aplicable al SGI de **LEGÁLITAS**.
- **O11: Defender los activos** frente a ataques internos o externos para que los eventos de seguridad no se conviertan en incidentes de seguridad o eventos de interrupción de actividad.
- **O12: Controlar el funcionamiento** de los controles y salvaguardas de seguridad de la información, así como de los planes de contingencia que se definan como respuesta a los escenarios de riesgo identificados.
- **O13: Mejora continua** del Sistema de Gestión Integrado (SGI) que se ha implantado para la gestión de ambos sistemas.

Para la consecución de los objetivos de Seguridad de la Información y Continuidad de Negocio anteriormente descritos, el SGI contará con el compromiso de la Dirección, expresado en la asignación de los recursos necesarios y en la supervisión activa del Sistema de Gestión.

2.3. Alcance

El alcance de esta política está definido en el PROCEDIMIENTO ALCANCE Y CONTEXTO DE LA ORGANIZACIÓN **PSGI-01**

2.4. Contexto

Para la definición del Alcance, detallado en el punto anterior, se ha tenido en cuenta el análisis de las partes interesadas y sus requisitos asociados, que quedan expuestos en el documento " Objetivos, alcance y contexto de la organización", dentro del cuerpo documental correspondiente al Sistema de Gestión Integrado de **LEGÁLITAS**.

2.5. Planificación

Las actuaciones a llevar a cabo para cumplir con la declaración de la política de seguridad de la información y continuidad de negocio pasan por la implantación, operación, mantenimiento y mejora de un Sistema de Gestión Integrado (SGI), que en todo momento debe estar alineado con esta política, que comprenda a ambos sistemas y bajo una única dirección.

En la fase de planificación se incluye, como punto fundamental, un estudio de la seguridad de la compañía y necesidades de continuidad de negocio a través de un análisis de riesgos (AARR) y Análisis de Impacto en Negocio (BIA), para el establecimiento del correspondiente plan de tratamiento de los riesgos no aceptados por la organización en materia de seguridad de la información y la definición de planes de contingencia con los que asegurar la continuidad del Negocio.

2.6. Implantación

La implantación del SGI es responsabilidad principal del Responsable del Sistema de Gestión Integrado apoyado en todo momento por personal técnico y con el total apoyo de la Gerencia de

LEGÁLITAS. Para la implantación se dispone de un comité de Sistemas de Gestión Integrado, que se ocupa de gestionar conjuntamente las normas ISO/IEC 27001:2013 e ISO/IEC 22301:2012.

En base a los resultados obtenidos en la fase de planificación, se implantan los controles de seguridad considerados como adecuados, además de operar los procedimientos del SGI para dar cumplimiento a las exigencias de los estándares ISO/IEC mencionados anteriormente.

El Comité del Sistema de Gestión Integrado (CSGI) definirá la estrategia que permita establecer los mecanismos técnicos y organizativos necesarios para detectar, prevenir y evitar los riesgos derivados de acciones humanas sobre sus Sistemas de Información, como pueden ser, fraude, sabotaje, robos, errores y otros. Estos mecanismos se establecerán de acuerdo con las indicaciones proporcionadas por las distintas áreas de negocio.

2.7. Revisión

La Política de Seguridad de la Información y Continuidad de Negocio, así como el SGI que la soporta serán revisados regularmente a intervalos planificados o si ocurren cambios significativos para asegurar la continua idoneidad, eficacia y efectividad de los mismas. De forma genérica son revisados anualmente en el proceso de auditoría interna y en la revisión por dirección del SGI.

Existen procesos de monitorización que aportan información sobre el correcto desempeño del SGI, gestionados a través de indicadores y métricas.

La Dirección también juega un importante papel en la revisión del sistema, realizando un profundo análisis del sistema y concretando posibles oportunidades de mejora.

2.8. Mejora

Las posibles mejoras de la Política de Seguridad de la Información y Continuidad de Negocio, así como del SGI que la mantiene, son establecidas bien durante las fases de revisión, bien en base a aportaciones que se consideren interesantes tanto de personal de **LEGÁLITAS** como de personal externo.

Dichas mejoras serán evaluadas por Comité del Sistema de Gestión Integrado y una vez estudiada su viabilidad, serán implementadas, operadas y mantenidas.

El Responsable del Sistema de Gestión Integrado debe gestionar las no conformidades, observaciones y oportunidades de mejora detectadas de forma que se establezcan las correspondientes acciones correctivas.

Todo el SGI se enmarca dentro del ciclo de Deming (ciclo PDCA), basado en la planificación de actividades, su implantación y operación, revisión y posterior mejora. Todo ello aplicado a la seguridad de la información y la continuidad de negocio.

Desde la Dirección de **LEGÁLITAS**, se considera que, a través de las acciones indicadas en todos los principios identificados en la presente Política, se asegurará el cumplimiento de los todos los objetivos de **LEGÁLITAS**, garantizando la buena imagen de la Compañía y asegurando la satisfacción de todos sus clientes, asumiendo que todas estas acciones permiten asegurar y cumplir con el compromiso de satisfacer las necesidades de todas las partes interesadas.

3. CUMPLIMIENTO NORMATIVO.

LEGÁLITAS identificará y mantendrá actualizada la relación de requisitos legales que le sean de aplicación en materia de seguridad de la información. De esta forma, podrá incluir en los contratos, licencias y acuerdos que establezca con terceros, el cumplimiento obligatorio por parte de éstos de las normas de seguridad corporativas, las cláusulas relativas a la propiedad intelectual, los derechos de explotación, confidencialidad y no divulgación, así como los requerimientos de seguridad exigibles por imperativos legales o regulatorios que sean de aplicación.

LEGÁLITAS, en cumplimiento de la normativa vigente, asegurará la confidencialidad, integridad y disponibilidad de los registros que pudieran ser requeridos por motivos legales y los protegerá frente a posibles pérdidas, destrucción o modificación.

4. INFORME DE SEGURIDAD.

El Comité del Sistema de Gestión Integrado (CSGI) establecerá los mecanismos y medios de reporte relacionado con la Seguridad de la Información y Continuidad de Negocio que puedan necesitar las partes interesadas, como pueden ser empleados, proveedores, accionistas, propietarios o autoridades y se reportará con la periodicidad que considere necesaria para cada uno de los grupos de interés que solicite la información.

5. EXCEPCIONES A LA POLÍTICA.

En caso de existir alguna excepción a esta política, se realizará una evaluación del riesgo específico e individualizado, examinándose las posibles consecuencias que dicha excepción pudiera conllevar. Estas excepciones serán presentadas por el Responsable del Sistema de Gestión Integrado al Comité del Sistema de Gestión Integrado quién se encargará de su revisión y aprobación, documentando en cada caso, los criterios para la resolución tomada al respecto.

6. INCUMPLIMIENTO A LA POLÍTICA.

El incumplimiento de esta política podrá dar lugar a que **LEGÁLITAS** inicie acciones disciplinarias y ejercite sus derechos mediante los procedimientos legales establecidos.

Firma del responsable