Política de Seguridad de la Información

versión	apartados modificados	razón de cambio	fecha
1.0	Todos	*Primera Versión*	Abril 2024

Elaborado por	Revisado por	Aprobado por
SECUREIT by LKS Next	**Responsable de Seguridad**	**Comité de Seguridad de la Información y Protección de Datos**

1. Índice

Contenido

2. Introducción

El objetivo del presente documento es regular la Política de Seguridad de la Información (PSI) de **Entelgy**, así como establecer la estructura Organizativa, para definirla, implantarla y gestionarla, y del marco tecnológico de la misma.

3. Alcance

Además de las obligaciones que se mencionan a lo largo de las políticas de seguridad, los responsables de seguridad de la información tienen también la obligación de controlar y coordinar: todos los sistemas, servicios y activos de Tecnologías de la información y la comunicación (de ahora en adelante TIC) de **Entelgy**, siendo extensible a todos los usuarios de los sistemas de la información, sin excepciones, debiendo ser conocida y cumplida por todos los usuarios de los sistemas de información y/o la información, incluido el soporte físico, internos y externos, con independencia de la posición, cargo y responsabilidad dentro de la Organización.

4. Misión

Entelgy somos The BusinessTech Consultancy, un acelerador global de la transformación para quienes necesitan seguir siendo competitivos en un mundo cambiante a gran velocidad.
Inspirando y aportando nuevas soluciones a los equipos con los que co-creamos y trabajamos. Ayudando a adoptar y hacer funcionar las nuevas tecnologías que impulsan sus retos, acompañándolos en su cambio, y ciberprotegiendo sus activos. Trabajamos a diario para alcanzar las oportunidades del mañana a la velocidad que necesitamos hoy, creando un futuro mejor para todos.
Con una visión global. Presentes en 8 países: Argentina, Brasil, Chile, Colombia, España, México, Perú y USA lo que nos permite dar una misma respuesta ante un mismo reto de negocio, de una manera global.

Entelgy somos diferenciales. Fundamentado en las personas y con un modelo empresarial de desarrollo sostenido a largo plazo, **Entelgy** cuenta con una oferta de alto valor y un gran reconocimiento del mercado gracias a la excelente labor de nuestros más de 2.000 profesionales cualificados y nuestros más de 300 clientes que nos han acompañado hasta hoy, de forma global, en *todo el mundo.* Nuestra cultura de innovación práctica nos incentiva a dar respuesta a

los *retos* del mañana a la velocidad que requiere "el hoy". Para ello contamos con el mejor y más excelente talento.

Para poder ofrecer el mayor valor a nuestros clientes, en **Entelgy** trabajamos bajo unos principios que nos hacen ser lo que somos:

- **Inspiradores & Proactivos**. Siempre buscando el mañana, anticipándonos a las necesidades futuras. Nuestra área de Innovación Sinapsis hace realidad nuestra visión de "aportar" más valor mediante la innovación, utilizando las capacidades tecnológicas de la compañía y generando soluciones que dan respuesta a los retos de negocio actuales. Nuestra presencia global en varios continentes nos proporciona una visión que nos permite anticiparnos a los nuevos retos del mundo.

- **Cercanos & Comprometidos**. Comprometidos con nuestros clientes y con nuestro talento. Con una presencia global queremos aportar a nuestros clientes sinergias, inspiración y equipos multidisciplinares para afrontar cualquier reto, en cualquier lugar.

- **Ágiles & Dinámicos**. Nos gusta hacer que las cosas sucedan, y que sucedan rápido, adaptándonos a una realidad cambiante. Desarrollamos alianzas y acuerdos con organizaciones innovadoras, porque creemos en la colaboración, la co-creación y la evolución de mano de los mejores especialistas en cada una de sus áreas. Por eso trabajamos cada día para ampliar nuestras alianzas estratégicas con los actores más importantes.

- **Expertos & Eficientes**. La excelencia por bandera. Desde sus comienzos, **Entelgy** ha apostado por incluir en sus modelos y marcos metodológicos estándares de reconocimiento internacional. Somos uno de los líderes de ámbito nacional que dispone de este conjunto de modelos de forma simultánea.

Todo ello trabajando para facilitar y acelerar el cambio de nuestros clientes a la velocidad que necesitan para alcanzar sus retos de negocio del mañana, hoy.

5. Objetivo

Esta política general de seguridad de la información cubre los siguientes objetivos:

- Establecer las expectativas de la Dirección con respecto al correcto uso que los usuarios hagan de los recursos de información de **Entelgy**, así como de las medidas que se deben adoptar para la protección de estos.

- Establecer para todo el personal de la organización la necesidad de la seguridad de la información y promover la comprensión de sus responsabilidades individuales.

- Determinar las medidas esenciales de seguridad de la información que **Entelgy** debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

- Proporcionar a todo el personal de **Entelgy** una herramienta que facilite la comunicación de incidentes en situaciones relacionadas con la preservación de la seguridad de la información.

5.1. Principios básicos.

5.1.1. Prevención

Todos los departamentos que integran **Entelgy** deben 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, deben implementar las medidas mínimas de seguridad determinadas por el ENS, 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 todos los usuarios, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, todos los departamentos que integran **Entelgy** 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.

5.1.2. 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 según lo establecido en el Artículo 10 del ENS.

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

5.1.3. Respuesta

Todos los departamentos que integran **Entelgy** deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

5.1.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, todos los departamentos que integran **Entelgy** deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

6. Requisitos de seguridad

Esta política de seguridad se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad	**Entelgy** considera fundamental establecer un proceso claro y estructurado para garantizar la seguridad de la Organización. Esto implica definir roles y responsabilidades, así como implementar políticas y procedimientos de seguridad, de acuerdo al procedimiento.
b) Análisis y gestión de los riesgos	La Organización debe realizar una evaluación constante de los posibles riesgos para identificar amenazas y vulnerabilidades. Luego, se deben implementar medidas para mitigar esos riesgos y verificar el correcto seguimiento e implementación de las mismas.
c) Gestión de personal	**Entelgy** debe asegurarse de que el personal esté adecuadamente capacitado en seguridad, así como establecer políticas y procedimientos para garantizar el cumplimiento de las normas de seguridad por parte de todos los empleados.
d) Profesionalidad	**Entelgy** establece a la necesidad de contar con personal calificado y ético en todas las funciones relacionadas con la seguridad, desde la planificación hasta la implementación y el mantenimiento.
e) Autorización y control de los accesos	La Organización establece controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a recursos y sistemas críticos.
f) Protección de las instalaciones	**Entelgy** implementa medidas físicas y tecnológicas para proteger las instalaciones de la Organización contra intrusiones y amenazas externas.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad	La Organización considera de especial relevancia el seleccionar cuidadosamente productos y servicios de seguridad confiables y adecuados para las necesidades específicas de **Entelgy**.
h) Mínimo privilegio	**Entelgy** establece el principio de otorgar a los usuarios solo los privilegios necesarios para realizar sus funciones, reduciendo así el riesgo de abuso o mal uso de los recursos.
i) Integridad y actualización del sistema	La Organización implementa medidas para garantizar la integridad de los sistemas y datos, así como mantenerlos actualizados con las últimas correcciones de seguridad.
j) Protección de la información almacenada y en tránsito	**Entelgy** debe implementar controles para proteger la información confidencial tanto mientras está en reposo como durante su transmisión.
k) Prevención ante otros sistemas de información interconectados	**Entelgy** considera de especial importancia tener en cuenta la seguridad de los sistemas interconectados para evitar posibles brechas de seguridad a través de estos puntos de conexión.
l) Registro de la actividad y detección de código dañino	La Organización implementa sistemas de registro y monitorización para detectar actividades sospechosas y posibles amenazas, así como contar con medidas para identificar y mitigar código malicioso.
m) Incidentes de seguridad	**Entelgy** establece un plan de respuesta a incidentes para manejar de manera efectiva y rápida cualquier violación de seguridad que ocurra.
n) Continuidad de la actividad	**Entelgy** implementa planes de continuidad del negocio para garantizar que la Organización pueda seguir funcionando en caso de un incidente de seguridad grave
o) Mejora continua del proceso de seguridad	La organización considera imprescindible velar por la mejora continua en el proceso integral de seguridad.

7. Estructura organizativa de seguridad

El documento "PR85-01 Roles y responsabilidades" establece la organización de seguridad de **Entelgy**. En dicho documento se nombra como Responsable de Seguridad a:

- Manuel Ruiz (CIO Global)

Como Delegado de Protección de Datos:

- Figura externalizada en Secure&IT Proyectos S.L.

Será responsable de la coordinación de la seguridad de la información, y único punto de contacto para los todos los Departamentos que integran **Entelgy** en esta materia.

8. Marco legal y regulatorio

Entelgy trata datos de carácter personal. El Sistema de Gestión de Privacidad, al que tendrán acceso sólo las personas autorizadas, recoge los tratamientos afectados y los responsables correspondientes.

Política de privacidad	https://www.entelgy.com/politica-de-privacidad

Todos los sistemas de información de **Entelgy** mencionadas se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos personales recogidos en el mencionado Sistema.
Asimismo, el marco legal y regulatorio en el que se desarrollan las actividades queda identificado en el anexo I de esta política de seguridad.

9. 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 la información manejada.

- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.

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

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La política de uso y seguridad de los sistemas de información estará a disposición de todos los usuarios que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

9.1. Estructuración de seguridad del sistema

De acuerdo a la clasificación de activos adoptada por la Organización, la documentación de procedimientos y registros del SGSIPD es gestionada de acuerdo al nivel de seguridad determinado por el aprobador del documento, a saber:

Confidencial (o restringido): dentro de este grupo se engloba toda la información que no debe ser accesible a todo el personal de la organización (está restringida a algunos profesionales). Puede ser de los siguientes tipos:

- información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidades de negocio, potencial de fraude o requisitos legales. Un ejemplo de este tipo de información son las decisiones del Comité de Dirección, Actas de estas reuniones, Información que contiene datos personales de nivel alto, etc.
- información interna a áreas o proyectos a los que debe tener acceso controlado un grupo reducido de personas y no toda la empresa y que debe ser protegida por su impacto en los intereses de la organización, de sus clientes o asociados y empleados. Un ejemplo de este tipo de información son planes estratégicos, datos de carácter personal de nivel

medio, políticas de RRHH, contratos laborales, curricula, informes de auditoría, etc.

Uso interno: Aquella información disponible al personal de la Organización, proveedores o terceros que precisen de información de **Entelgy** para el desempeño de sus funciones (procedimientos, manuales, instrucciones del sistema de gestión, etc.), y que no ha sido clasificada como confidencial o pública.

Pública: Información de la página web, folletos publicitarios, presentaciones de productos y servicios, etc.

10. Obligaciones de los usuarios

Todos los miembros de **Entelgy** definidos en el alcance tienen la obligación de conocer y cumplir la Política de Seguridad de la Información y las diferentes normativas en materia de seguridad de la información, siendo responsabilidad del Comité de Seguridad de la Información y Protección de Datos disponer los medios necesarios para que la información llegue a los afectados.
Todos los miembros de **Entelgy** con responsabilidad sobre la información atenderán a una sesión 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 previamente indicados.
Los usuarios 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 o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

11. Terceras partes

Cuando **Entelgy** 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 creados y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando **Entelgy** utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que involucre 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.

12. Aprobación y entrada en vigor

Texto aprobado por el Comité de Seguridad de la Información y Protección de Datos el 8 de mayo de 2024.

Esta Política de Seguridad de la Información es efectiva desde su fecha de publicación y hasta que sea reemplazada por una nueva Política.

13. Anexo I: Marco legal y regulatorio aplicable

LEGISLACION	AMBITO DE APLICACIÓN
Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.	España
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	Europa
Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos de Carácter Personal y garantía de los derechos digitales.	España
Real Decreto 1720/2007, de 21 de diciembre	España
Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.	España
Código Penal art. 199 su sucesivos	España
Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia	España
Ley 24/2015, de 24 de julio, de Patentes.	España
Reglamento (UE) 910/2014 del parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior.	Europa
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.	España
Directiva 1999/93/CE, por la que se establece un marco comunitario para la firma electrónica	Europa
Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social.	España
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.	España
Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias	España