POLÍTICA DE **SEGURIDAD DE LA INFORMACIÓN**

CONGENIA INTEGRACIÓN S.L.

ENTRADA EN VIGOR

Esta Política se Seguridad de la Información es efectiva desde la misma fecha de aprobación y hasta que sea reemplazada por una nueva Política.

INTRODUCCIÓN

CONGENIA INTEGRACIÓN S.L. depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados. La información es un activo esencial de gran valor para el desarrollo de la actividad de CONGENIA. Dicho activo debe ser adecuadamente protegido; en este caso, a través de la Seguridad de la Información, con el objetivo de asegurar la calidad y continuidad de la actividad y servicios prestados, además de garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS, en adelante) operado por el Real Decreto 311/2020 de 3 mayo, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC. Dichos departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

PREVENCIÓN

Los departamentos 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 los departamentos 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 todo el personal, deben estar claramente definidos y documentados.

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

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

DETECCIÓN

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

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.

RESPUESTA

Los departamentos 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).

RECUPERACIÓN

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

ALCANCE

El alcance de nuestro **SG** se ha determinado teniendo en cuenta los factores externos e internos y los requisitos de las partes interesadas, así como los requisitos legales. Teniendo en cuenta todo lo mencionado, el alcance del **SG** comprende**:**

- *La gestión de la seguridad de la información que da soporte a todos los procesos de la organización (planificación estratégica, creación de nuevos clientes, introducción de funcionalidades, controles de acceso, incorporación de contenido, gestión de altas de usuarios, comunicaciones y contraseñas, configuración de copas de seguridad, asistencia técnica a usuarios y disponibilidad de la información) prestados desde los puestos en remoto del personal cuya sede se ubica en Arturo Campión, 46 – Esc. 3 – Bajo A Guipúzcoa Donostia-San Sebastián 20018, según la Declaración de Aplicabilidad vigente (Edición 00 de junio de 2025). El ámbito de aplicación se extiende a todos los miembros de* ***CONGENIA INTEGRACIÓN S.L.*** *determinados dentro del alcance, así como todo aquel personal contratado, subcontratado, agentes vinculados, socios, colaboradores y demás personas físicas y jurídicas que actúen de forma autorizada en nombre o por cuenta de nuestra organización."*

MISIÓN

CONGENIA INTEGRACIÓN S.L., organización dedicada al desarrollo de cursos en línea gestionados a través de una plataforma online propia, tiene como objetivo empoderar a las personas a través del aprendizaje online de calidad, ofreciendo experiencias formativas accesibles, efectivas y motivadoras mediante una plataforma amigable y contenidos atractivos y originales, con especial foco en la enseñanza de idiomas y el desarrollo de competencias clave que potencien la interculturalidad.

VISIÓN

Ser un referente en el ámbito de la formación online, reconocidos por la innovación pedagógica, la calidad de nuestros contenidos y la capacidad para adaptarnos a las necesidades específicas de cada uno de nuestros clientes, impulsando el crecimiento personal y profesional de nuestros usuarios finales en cualquier lugar y momento.

VALORES

Calidad educativa: Diseñamos contenidos rigurosos, actualizados y orientados al aprendizaje significativo.

Innovación: Apostamos por soluciones creativas y tecnológicamente avanzadas que mejoren la experiencia del usuario.

Accesibilidad: Promovemos una formación inclusiva y flexible, sin barreras de tiempo ni lugar.

Autonomía del alumno: Fomentamos la autoformación y la metodología learning by doing.

Compromiso con el aprendizaje continuo: Creemos en el poder transformador de la educación a lo largo de toda la vida.

Cercanía y humanidad: Aunque trabajamos en entornos digitales, situamos siempre a las personas en el centro de cualquier proceso.

Confidencialidad y privacidad educativa: Garantizamos que la información personal, académica y profesional de nuestros usuarios esté protegida frente a accesos no autorizados.

Disponibilidad continua del servicio formativo: Nos aseguramos de que los contenidos educativos estén accesibles en todo momento.

Integridad de los contenidos y datos: Trabajamos para que toda la información publicada, compartida o generada por nuestros usuarios en la plataforma sea veraz, íntegra y no haya sido alterada sin autorización, promoviendo la confianza en el proceso formativo.

Trazabilidad y control de accesos: Implementamos mecanismos que permiten registrar, auditar y supervisar los accesos y acciones dentro de nuestros sistemas, garantizando la trazabilidad de las actividades y fortaleciendo la transparencia operativa.

Cumplimiento normativo y seguridad legal: Actuamos conforme a los principios del Esquema Nacional de Seguridad y otras normativas relevantes (como el RGPD), integrando la seguridad jurídica y tecnológica como pilar esencial de nuestro modelo educativo.

MARCO NORMATIVO

El marco normativo de las actividades de CONGENIA INTEGRACIÓN SL se encuentra en el ámbito que se expone a continuación, según jerarquía jurídica del ordenamiento jurídico estatal:

- **Ley Orgánica 3/2018** (LOPDGDD) y RGPD: encargada del tratamiento, DPD, medidas técnicas, EIPD, contrato con AA.PP.
- **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común: garantiza la integridad, trazabilidad y autenticación en procesos electrónicos.
- **Ley 40/2015**, de 1 de octubre, de Régimen Jurídico del Sector Público: impone la necesidad de interoperabilidad y seguridad en los sistemas usados por la administración. Obliga al cumplimiento del Esquema Nacional de Seguridad (ENS).
- **Ley 9/2017**, de Contratos del Sector Público (LCSP) Cumplir pliegos, solvencia, auditoría, documentación contractual.
- **Real Decreto 311/2022** – Esquema Nacional de Seguridad (ENS) Cumplir ENS (análisis de riesgos, medidas técnicas, conformidad/certificación).

Del mismo modo, se tendrán en cuenta las modificaciones y derogaciones de dicha normativa que afecten a esta Política de Seguridad de la Información

ORGANIZACIÓN DE LA SEGURIDAD

Tomando en cuenta el contexto y organigrama de la organización, se acuerda establecer la designación de los siguientes roles:

Rol (ENS)	Persona designada	Cargo en la organización
Responsable de la Información	*José María Muñoz Nájera*	Director
Responsable de Seguridad	*José María Muñoz Nájera*	Director
Responsable del Servicio	*Pello Altadill Izura*	Responsable de Desarrollo
Responsable del Sistema	*Pello Altadill Izura*	Responsable de Desarrollo

El Director asume el rol de **Responsable de la Seguridad**, asumiendo que es quien tiene la autoridad ejecutiva de exigir el cumplimiento del ENS; además del rol de **Responsable de la Información**, en tanto que es quien asume las decisiones estratégicas sobre los servicios prestados a los clientes y cuenta con un conocimiento y visión global del valor de la información en la organización.

El **Responsable de Desarrollo** asume el rol de **Responsable del Servicio**, ya que gestiona, entre otros aspectos, la disponibilidad, actualización, mantenimiento y nuevas funcionalidades del sistema; garantizando, de esta manera, el funcionamiento óptimo del servicio. Del mismo modo, asume el rol de Responsable del Sistema ya que es el encargado de la infraestructura técnica como las copias de seguridad, el control de accesos y el cifrado.

El **Comité de Seguridad de la Información** estará formado por el Director y el Responsable de Desarrollo, encargado de coordinar la seguridad de la información de la organización y de promover la mejora continua.

FUNCIONES Y RESPONSABILIDADES

Cada responsable asume las funciones y responsabilidades concretas (dentro del alcance de la organización) identificadas en el marco del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, así como en la "*Guía de Seguridad (CCN-STIC-801)*

ESQUEMA NACIONAL DE SEGURIDAD RESPONSABILIDADES Y FUNCIONES"[1]; entre las cuales, se encuentran:

Rol (ENS)	Funciones y responsabilidades
Responsable de la Información	▪ Establecer los requisitos de una información en materia de seguridad. ▪ Determinar los requisitos de la información tratada: clasificación de información, gestión de ciclo de vida de la información, protección de datos personales… ▪ Asumir la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. ▪ Asumir la responsabilidad de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad. ▪ Establecer los requisitos de la información en materia de seguridad. En terminología del ENS, la potestad de determinar los niveles de seguridad de la información.
Responsable de Seguridad	▪ Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. ▪ Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Organización. ▪ Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. ▪ Impulsar y supervisar, de manera continua, la implementación y eficacia del Sistema en los distintos ámbitos de la organización. ▪ Asegurarse que se establecen, implementan y mantienen los procesos necesarios para el Sistema de Gestión de la Seguridad de la Información. ▪ Asegurar que se proporciona apoyo formativo continuo a los miembros de la organización, para garantizar que todos los miembros relevantes son formados con regularidad. ▪ Promover la inclusión de las responsabilidades necesarias en materia de seguridad de la información en las descripciones de puestos de trabajo y en los procesos de gestión del desempeño de los miembros de la organización. ▪ Poner en marcha un sistema de información y documentación de cumplimiento de los requisitos de la norma de referencia. ▪ Adoptar e implementar procesos para gestionar la información. ▪ Establecer indicadores de desempeño de cumplimiento y medir el desempeño en la gestión de la seguridad de la información.

[1] Sin perjuicio de otras funciones que puedan ser encomendadas por la Dirección y que en su caso se reflejarán debidamente en el Sistema.

	▪ Analizar el desempeño para identificar la necesidad de acciones correctivas. ▪ Identificar y gestionar los riesgos de seguridad de la información, incluyendo los relacionados con los socios de negocio. ▪ Asegurar que el Sistema se revisa a intervalos planificados. ▪ Proporcionar asesoramiento y orientación al personal sobre el SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. ▪ Asegurar que se proporciona a los empleados acceso a los recursos necesarios para el cumplimiento de los requisitos. ▪ Asegurarse de que el SISTEMA es conforme con los requisitos del Esquema Nacional de Seguridad.
Responsable del Servicio	▪ Establecer los requisitos de un servicio en materia de seguridad. ▪ Determinar los requisitos de los servicios prestados. ▪ Definir las necesidades de seguridad de los servicios contemplados en el análisis de riesgos para cada una de las diferentes dimensiones de seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente. ▪ Colaborar en el análisis de impacto de los incidentes que puedan acontecer.
Responsable del Sistema	▪ Reportar al responsable de Seguridad. ▪ Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos (esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el Responsable de la Seguridad, antes de ser ejecutad). ▪ Por sí mismo o a través de recursos propios o contratados, desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo pudiendo delegar en administradores u operadores bajo su responsabilidad.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Director y el Responsable de Desarrollo la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por la Dirección y ampliamente difundida a fin de dar conocimiento de esta a todas las partes interesadas, tanto internas como externas.

DATOS DE CARÁCTER PERSONAL

CONGENIA INTEGRACIÓN S.L. trata datos de carácter personal. La ubicación que contenga dichos datos será accesible únicamente por las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de CONGENIA INTEGRACIÓN S.L. se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

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
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC 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 de Seguridad de la Información complementa las políticas de seguridad de CONGENIA INTEGRACIÓN S.L., en diferentes materias, que serán ampliamente difundidas entre las partes interesadas correspondientes:

- Política control accesos
- Política gestión contraseñas
- Política controles criptográficos
- Política uso aceptable de activos
- Política de desarrollo

Esta Política (PO 00 POLÍTICA DE SEGURIDAD) se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. La normativa de seguridad estará disponible en la página web de la organización (https://www.congenia.eu/es/).

OBLIGACIONES DEL PERSONAL

Todos los miembros de CONGENIA INTEGRACIÓN S.L. tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad de la Dirección disponer los medios necesarios para que la información llegue a los afectados. Todos los miembros de la organización 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 de la organización, 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 o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

TERCERAS PARTES

Cuando CONGENIA INTEGRACIÓN S.L. 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 TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando CONGENIA INTEGRACIÓN S.L. 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 ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

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

15978993L JOSE MARIA MUÑOZ (R: B20536215)

Firmado digitalmente por 15978993L JOSE MARIA MUÑOZ (R: B20536215)
Fecha: 2025.06.23 16:39:13 +02'00'