APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 02 de julio de 2026 por **DIRECCIÓN**.
Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

INTRODUCCIÓN

CHEIL SPAIN 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.
El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.
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, 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.
Los 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

Esta política se aplica a todos los sistemas TIC de **CHEIL SPAIN** y a todos los miembros de la CHEIL SPAIN, sin excepciones.

MISIÓN

CHEIL SPAIN tiene como misión proporcionar soluciones integrales de marketing, publicidad, comunicación, creatividad y transformación digital que aporten valor a sus clientes, mediante el desarrollo y ejecución de estrategias innovadoras, campañas de comunicación y servicios tecnológicos adaptados a las necesidades del negocio.

La organización orienta su actividad a ofrecer servicios de alta calidad, garantizando el cumplimiento de los requisitos contractuales, legales y reglamentarios aplicables, así como la protección de la información gestionada durante la prestación de sus servicios.

En este contexto, **CHEIL SPAIN** considera la seguridad de la información un elemento estratégico para preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los sistemas que soportan su actividad, contribuyendo a la continuidad del negocio, a la confianza de sus clientes y colaboradores y al cumplimiento del Esquema Nacional de Seguridad y del resto de la normativa aplicable.

MARCO NORMATIVO

A continuación, se detallan todos los requisitos legales aplicables a la organización:

- Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad
- Ley 40/2015, de Régimen Jurídico del Sector Público
- Reglamento (UE) 2016/679 (RGPD)
- Ley Orgánica 3/2018 (LOPDGDD)
- Ley 34/2002 (LSSI-CE)
- Reglamento (UE) 910/2014 (eIDAS)
- Reglamento (UE) 2024/1183 (eIDAS 2)
- Directiva NIS2 (UE) 2022/2555
- Reglamento (UE) 2022/2554 (DORA)
- Ley 9/2017 de Contratos del Sector Público
- Ley 39/2015 del Procedimiento Administrativo Común
- Ley 56/2007 de Medidas de Impulso de la Sociedad de la Información
- Real Decreto Legislativo 2/2015 (Estatuto de los Trabajadores)
- Ley 31/1995 de Prevención de Riesgos Laborales
- Real Decreto 171/2004
- Real Decreto 1215/1997
- Ley 10/2021 de Trabajo a Distancia
- Ley 1/2019 de Secretos Empresariales
- Código Penal (artículos relativos a delitos informáticos y revelación de secretos)
- Real Decreto Legislativo 1/1996 (Ley de Propiedad Intelectual)

- Ley 11/2022 General de Telecomunicaciones

ORGANIZACIÓN DE LA SEGURIDAD
COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad TIC estará formado por:

- Responsable de la Información:	Marcos Velasco
- Responsable del Servicio:	Marcos Velasco
- Responsable de Seguridad:	Óscar López
- Responsable del Sistema:	Óscar López

ROLES: FUNCIONES Y RESPONSABILIDADES

La designación de los roles y responsabilidades definidos en la presente acta se ha realizado tomando como referencia la Guía CCN-STIC 801 "Responsabilidades y Funciones", adaptando su contenido a la estructura organizativa y a las necesidades de la organización, especialmente en lo relativo a la definición de funciones del Responsable de Seguridad y su relación con el Comité de Seguridad.

Sus funciones quedan reflejadas en el Acta de Comité de Seguridad con fecha 02/07/2026.

PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por Dirección a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.
El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por **DIRECCIÓN** y difundida para que la conozcan todas las partes afectadas.

DATOS DE CARÁCTER PERSONAL

CHEIL SPAIN trata datos de carácter personal. Todos los sistemas de información de **CHEIL SPAIN** se ajustarán a los niveles de seguridad requeridos por la normativa estatal y europea para la naturaleza y finalidad de los datos de carácter personal almacenados y tratados en los sistemas de **CHEIL SPAIN**.

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 **CHEIL SPAIN** en diferentes materias:

- Política de Control de Accesos
- Política de Gestión de Contraseñas
- Política de Controles Criptográficos
- Política de Uso Aceptable de Activos
- Year 2026 Global Management Guideline (IT)

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

OBLIGACIONES DEL PERSONAL

Todos los miembros de **CHEIL SPAIN** 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 TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de **CHEIL SPAIN** 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 **CHEIL SPAIN**, 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 **CHEIL SPAIN** 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 **CHEIL SPAIN** 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.

En Madrid, a 02/07/2026
DIRECCIÓN