POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CONTROL DE MODIFICACIONES			
Edición	Fecha	Aptdo.	Descripción de la Modificación
00	06/02/2020		Edición Inicial del sistema de Gestión UNE-EN ISO 27001:2017
01	05/04/2021		Aclaración en punto 4 sobre los requisitos de mejora continua y cumplimiento de requisitos legales

Elaborado:	Revisado y Aprobado:
Responsable del Sistema	Dirección

Contenido

1. VIGENCIA

La presente Política ha sido aprobada por el comité de seguridad de CONNECTION SOFT SERVICE, S.L.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación y las versiones anteriores quedarán anuladas por la última versión de esta Política.

2. INTRODUCCIÓN

CONNECTION SOFT SERVICE, S.L. es consciente de que la seguridad de la información es una necesidad fundamental y que es necesario garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con agilidad a los incidentes.

Por ello, los sistemas TIC 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.

2.1. OBJETIVO

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 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.

3. ALCANCE

Esta política se aplica a todos los sistemas TIC de CONNECTION SOFT SERVICE, S.L. y a todos los miembros de la compañía, sin excepciones.

4. DIRECTRICES DE OBLIGADO CUMPLIMIENTO

Los departamentos y sistemas deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

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. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para los sistemas. Para ello se deben implementar las medidas mínimas de seguridad necesarias, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Como medidas preventivas, se deben llevar a cabo las siguientes:

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria, que permita adecuar su eficacia a la continua evolución de los sistemas de protección frente a nuevos ataques o riesgos.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Se establecerán mecanismos de monitorización, detección, análisis y reporte que lleguen a los responsables regularmente o cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.

Además, para garantizar la disponibilidad de los servicios críticos, se desarrollarán planes de continuidad de los sistemas TIC como parte del plan general de continuidad de negocio y actividades de recuperación.

La organización se compromete a dar cumplimiento a los requisitos legales aplicables, los compromisos adquiridos con los clientes y toda aquella reglamentación, normas internas o pautas de actuación a los que se someta la empresa.

De igual modo, la empresa se compromete a aplicar la presente política, y el propio sistema de gestión, como base de la mejora continua de sus actividades en materia de Seguridad de la Información.

5. RESPONSABILIDADES Y FUNCIONES

El Comité de Seguridad Corporativa estará formado por:

- Dirección
- El responsable del SGI
- El responsable de Administración

El Secretario del Comité de Seguridad será el responsable del SGI y tendrá las funciones de coordinar y organizar las reuniones del comité.

El Comité de Seguridad Corporativa tendrá las siguientes funciones:

- Coordinar todas las funciones de seguridad de la compañía.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Elaboración y aprobación de la Política Global de Seguridad.
- Aprobar las políticas de seguridad de las diferentes áreas.
- Coordinar y aprobar las propuestas recibidas de proyectos de seguridad presentados.
- Estudiar las diferentes inquietudes de la Alta Dirección.
- Recabar de los responsables de seguridad informes regulares del estado de la seguridad de la organización y de los posibles incidentes.
- Coordinar y dar respuesta a las inquietudes transmitidas a través de los responsables de la Seguridad.

6. DATOS DE CARÁCTER PERSONAL

CONNECTION SOFT SERVICE, S.L. trata datos de carácter personal. El Documento de Seguridad y el Registro de Tratamiento, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de CONNECTION SOFT SERVICE, S.L. se ajustarán a los niveles de seguridad requeridos por las normativas y reglamentos en protección de datos para la naturaleza y finalidad de los datos de carácter personal recogidos.

7. GESTIÓN DE RIESGOS

Se llevará a cabo un análisis de riesgos TIC de todos los sistemas sujetos a esta Política, que permitirá evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá regularmente y al menos una vez al año.

8. DESARROLLO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de CONNECTION SOFT SERVICE, S.L. en diferentes materias. Entre las políticas de seguridad que se incluyen en la compañía, se encuentran las siguientes:

- Política Clasificación y manejo de la información
- Política de uso de dispositivos móviles
- Política de uso aceptable
- Política para cuentas y contraseñas
- Política de uso de medios sociales

9. OBLIGACIONES DEL PERSONAL

Todos los miembros de CONNECTION SOFT SERVICE, S.L. tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Política de uso aceptable, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de CONNECTION SOFT SERVICE, S.L., en particular a los de nueva incorporación.

10. TERCERAS PARTES

Cuando CONNECTION SOFT SERVICE, S.L. preste servicios a otras compañías o maneje información de otras compañías, 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 CONNECTION SOFT SERVICE, S.L. utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Política de uso aceptable que aplique a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha política, 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.