POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1 APROBACIÓN Y ENTRADA EN VIGOR

La presente Política ha sido aprobada el día 24 de Febrero de 2025 por la Alta Dirección de IATEL.

2 INTRODUCCIÓN

IATEL 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, autenticidad, trazabilidad 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 celeridad a los incidentes.

2.1 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. 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.

2.2 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.

2.3 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 organismos de naturaleza pública a los que preste servicios.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CCN-CERT en el sector público, INCIBE en el sector privado).

2.4 Conservación

Para garantizar la conservación de los datos e información en soporte electrónico, los departamentos deben desarrollar políticas de retención y conservación basados, en primer lugar, en exigencias legales o plazos de responsabilidad. Y, en segundo lugar, en criterios internos justificados para la conservación finita de los datos e información.

3 OBJETIVO DE LA SEGURIDAD DE LA INFORMACIÓN

- Objetivos corporativos o estratégicos: Metas de alto nivel alineadas con la visión, misión y estrategia general de la organización.
  - Asegurar una alta disponibilidad de los servicios.
  - Fortalecer los sistemas frente ataques externos.
  - Reducir los tiempos de restauración de datos y servicios.
  - Mejorar el nivel de compromiso de la empresa con la seguridad.
  - Poder prestar servicios a la Administración Pública.
- Objetivos operativos: Metas específicas y tácticas enfocadas en la implementación práctica y diaria de controles y medidas de seguridad.
  - Hacer pruebas de restauración anuales.
  - Reducir el número de incidencias de seguridad.
  - Crear un boletín corporativo de ciberseguridad.
  - Implantar y certificar ENS.

4 ALCANCE

Los sistemas de información que dan soporte a las actividades de:

A) La instalación y el mantenimiento de elementos, equipos y sistemas de energía, trasmisión, radio y conmutación para telecomunicaciones fijas y móviles.

B) El diseño, la ejecución, el mantenimiento de infraestructuras y obra civil para estaciones de telecomunicaciones.

C) El diseño, la producción, la integración, el montaje, el conexionado y mantenimiento de contenedores para telecomunicaciones v de cuadros eléctricos.

La categoría objetivo de referencia que se determina para los sistemas de información descritos en este Alcance General es: NIVEL MEDIO.

5 MARCO NORMATIVO.

IATEL está sujeto, a título enunciativo y no limitativo, a las siguientes normativas y regulaciones:

- 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 (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- 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. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

6 CUMPLIMIENTO DE ARTÍCULOS DEL ENS

IATEL, para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica, que recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral (artículo 6), seguridad por defecto y mínimo privilegio (artículo 20)

La seguridad constituye un proceso integrado por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad a IATEL, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuente de riesgo para la seguridad.

Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Vigilancia continua y reevaluación periódica (artículo 10) e integridad y actualización del sistema (Artículo 21)

IATEL, ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Asimismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Finalmente, la vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta, y la evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Gestión de personal (artículo 15) y profesionalidad (artículo 16)

Todos los miembros de IATEL dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa

de concienciación continua para atender a todos los miembros, 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.

Gestión de la seguridad basada en los riesgos (artículo 7) y análisis y gestión de riesgos (artículo 14)

Todos los sistemas afectados por esta Política de Seguridad, así como todos los tratamientos de datos personales, deberán ser objeto de 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 cambien la información manejada y/o los servicios prestados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.
- El Responsable de Seguridad del ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

Incidentes de seguridad (artículo 25), prevención, detección, respuesta y conservación (artículo 8)

IATEL, ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubren los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, IATEL, implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales, se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

IATEL, establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un 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 (CCN-CERT en el sector público, INCIBE en el sector privado).
- Para garantizar la disponibilidad de los servicios, IATEL, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa (artículo 9) y prevención ante otros sistemas interconectados (artículo 23)

IATEL, ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

- Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
- Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
- Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Función diferenciada (artículo 11) y organización e implantación del proceso de seguridad (artículo 13)

IATEL, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de “ORGANIZACIÓN DE LA SEGURIDAD” del presente documento.

Autorización y control de los accesos (artículo 17)

IATEL, ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones (artículo 18)

IATEL, ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Protección de la información almacenada y en tránsito (artículo 22) y continuidad de la actividad (artículo 26)

IATEL, ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, smartphones, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

Se han desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los archivos electrónicos producidos en el ámbito de las competencias de IATEL, De igual modo, se han implementado mecanismos de seguridad en base a la naturaleza del soporte en el que se encuentren los documentos, para garantizar que toda información relacionada en soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad (artículo 24)

IATEL, ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

Mejora continua del proceso de seguridad (artículo 27)

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

7 ORGANIZACIÓN DE LA SEGURIDAD

7.1 Comité de Seguridad de la Información:

Formado por el CEO, el responsable IT, el responsable de sistemas, el responsable de RRHH, el responsable de sistemas integrado de gestión y el responsable de desarrollo de software. Tiene las siguientes funciones:

- Atender las solicitudes, en materia de Seguridad de la Información, de IATEL y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.

• Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes áreas o departamentos.

• Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:

o Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

o Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.

o Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

o Realizar un seguimiento de los principales riesgos residuales asumidos por IATEL y recomendar posibles actuaciones respecto de ellos.

o Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.

o Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el CEO.

o Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.

o Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.

o Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.

o Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.

o Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de IATEL en materia de seguridad de la Información.

7.2 Roles: Funciones y responsabilidades

Responsable de la Información:

- Determinar los requisitos (de seguridad) de la información tratada.

- Valorar las consecuencias de un impacto negativo sobre la seguridad de la información, se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

Responsable del Servicio:

- Determinar los requisitos (de seguridad) de los servicios prestados.
- Incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valorar las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

Responsable de la Seguridad:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Verificar, validar y actualizar la normativa vigente aplicable al ENS y proceder a su archivado en el repositorio correspondiente asó como en la Política de Seguridad de la Información del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Verificar, validar y actualizar la normativa vigente aplicable al ENS y proceder a su archivado en el repositorio correspondiente, así como esta Política de Seguridad de la información.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.

- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

Responsable del Sistema:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Prestar al responsable de Seguridad de la Información y/o el Comité de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
- Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.
    - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
    - Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
    - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
    - Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

- Cuando la complejidad del sistema lo justifique, el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

Administrador de Seguridad:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de la Seguridad o al Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

7.3 Política de seguridad de la información

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de esta.

8 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.

9 NOTIFICACIÓN DE INCIDENTES

De conformidad con lo dispuesto en el artículo 25 del RD 311/2022, IATEL notificará a los organismos competentes aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas recogidos.

10 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de IATEL en diferentes materias:

- Procedimientos de seguridad informática internos.
- Procedimientos de protección de datos personales internos.
- Procedimientos operativos internos con incidencia en la seguridad de la información.

La normativa de seguridad estará disponible electrónicamente en el intranet de IATEL.

11 OBLIGACIONES DEL PERSONAL

Todos los miembros de IATEL 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.

12 TERCERAS PARTES

Cuando IATEL preste servicios a organismos de naturaleza pública o maneje información de organismos de naturaleza pública, 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 IATEL subcontrate servicios con terceros o ceda información a terceros, en el marco de una prestación de servicios a organismos de naturaleza pública, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe 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.

13 MEJORA CONTINUA

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas. Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

- Revisión de la Política de Seguridad de la Información.
- Revisión de los servicios e información y su categorización.
- Ejecución con periodicidad anual del análisis de riesgos.
- Realización de auditorías internas o, cuando procedan, externas.
- Revisión de las medidas de seguridad.
- Revisión y actualización de las normas y procedimientos.

14 RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre los diferentes responsables de información o de servicio que componen la estructura organizativa de la Política de Seguridad de la Información, éste será resuelto por el superior jerárquico de los mismos, pudiendo participar en la resolución y mediación el responsable de Seguridad de la Información. En caso de no llegar a un acuerdo, se elevará para su resolución en última instancia al Comité de Seguridad de la Información.