LOGICALIS
Architects of Change

ENS07 – Política de seguridad

Índice de modificaciones

Edición	Fecha	Modificaciones	Páginas modificadas
1	05/08/2022	Creación del documento	Todas
2	14/02/2024	Se indica el servicio al que aplica. Se añade el apartado 1.1 "Identificación" Se actualiza referencia ENS. Supresión de la lista de normativas aplicables, que se sustituye por referencia al doc: *Cumplimiento de los requisitos legales y contractuales.*	4, 5 y 7.
3	03/04/2024	Se amplía punto 5 RGPD, se modifica alcance.	5 y 7
4	02/06/2025	Nueva plantilla (actualización formato) y correcciones. (*En cursiva se reflejan los cambios)*	Todas

Índice

1 INTRODUCCIÓN 4
1.1. Identificación 4
1.2. Prevención/ Protección 4
1.3. Detección 5
1.4. Respuesta 5
1.5. Recuperación 5
2 ALCANCE 5
3 OBJETIVOS 6
4 MARCO LEGAL Y REGULATORIO 7
5 DATOS DE CARÁCTER PERSONAL 7
6 DATOS DE CARÁCTER PERSONAL 8
7 ROLES DE SEGURIDAD 8
7.1. Responsable de la Seguridad de la Información 8
7.2. Responsable de la Información 9
7.3. Responsable de los Servicios 9
7.4. Responsable de los Sistemas 9
7.5. Delegado de Protección de Datos 10
7.6. Comité de seguridad de la información 11
8 OBLIGACIONES DEL PERSONAL 12
9 NOTIFICACIÓN DE INCIDENTES 12
10 DIRECTRICES DE ESTRUCTURACIÓN, GESTIÓN Y ACCESO A LA DOCUMENTACIÓN 12
11 TERCERAS PARTES 13
12 MEJORA CONTINUA 13

1 Introducción

Logicalis como proveedor internacional de servicios de tecnología de la información está comprometido con la seguridad de la información y privacidad de datos *personales*, tanto a nivel interno y organizativo, como a nivel externo *sobre* partes interesadas. En este sentido, Logicalis *prioriza disponer de* determinados sistemas y recursos que permitan ofrecer el rendimiento esperado para que todas las actividades sean realizadas con la mayor garantía posible, todo ello con el objetivo de garantizar la eficacia y *eficiencia de los servicios* a los que resulta de aplicación esta política de conformidad con el alcance.

La seguridad de la información permite la continuidad de las actividades de LOGICALIS, reduciendo al mínimo el riesgo de daño mediante la prevención de incidentes de seguridad y minimizando su impacto potencial.

La presente política trata de proteger los activos de información de la organización contra todas las amenazas internas, externas, deliberadas o accidentales, garantizando:

- Confidencialidad de la información;
- Integridad de la información;
- Disponibilidad de información para los procesos de negocio;
- Trazabilidad de la información
- *Autenticidad* de la información

Logicalis consciente de la importancia que tiene la seguridad de la información para el desarrollo de su negocio, ha decido implantar un sistema de gestión suscribiendo la presente política, que se alinea con las directrices del grupo Logicalis.

Es responsabilidad de Logicalis establecer y comunicar a todos los empleados las políticas y procedimientos necesarios.

1.1. Identificación

Resulta fundamental identificar funciones y responsabilidades de proveedores, empleados y terceros que de forma autorizada tengan acceso a la información, así como aquellas actuaciones frente ataques que afecten al sistema de información. Es esencial fundamentar la seguridad de la información en la identificación y análisis de las principales amenazas, con el fin de gestionar los riesgos a través de la evaluación y planificación. La función de identificar tiene como función determinar:

- Vulnerabilidades y amenazas potenciales para los activos.
- Activos de información de la empresa (hardware, software, datos y redes).
- Requisitos legales necesarios para la empresa en relación con la ciberseguridad.
- Objetivos de la empresa con respecto a la ciberseguridad.

1.2. Prevención/ Protección

Los empleados de Logicalis deben evitar, y en su caso prevenir, que cualquier información relacionada con los servicios puede verse perjudicada por incidentes de seguridad. Para ello Logicalis debe implementar las medidas de seguridad necesarias, así como cualquier control mediante una evaluación

de amenazas y riesgos. Los controles, roles y responsabilidades deben estar definidos y documentados. En resumen, como puntos principales Logicalis desarrolla su actuación en base a:

- Evaluar y autorizar los sistemas antes de su entrada en producción.
- Realizar de manera regular evaluaciones de seguridad
- Contratar evaluaciones por parte de terceros

1.3. Detección

Dado que existe la posibilidad de que los servicios puedan degradarse a causa de la materialización de incidentes, estos deben ser monitorizados de tal manera que puedan detectarse anomalías en los distintos niveles de prestación de los servicios. Se crearán mecanismos de detección, análisis y reporte para que todas las partes interesadas estén informadas cuando se produzca alguna desviación significativa.

1.4. Respuesta

Logicalis establecerá:

- Medios adecuados para responder a los incidentes de seguridad.
- Un punto de contacto para aquellas comunicaciones relacionadas con incidentes de seguridad
- Procedimientos para intercambiar la información relacionada con cada incidente incluyendo como partes interesadas a los organismos oficiales.

1.5. Recuperación

Logicalis *dispone de* planes de continuidad *internos que cubren diferentes contingencias* para asegurar la disponibilidad de aquellos servicios considerados críticos.

2 Alcance

El Alcance del ENS (Real Decreto 311/2022, de 3 de mayo), por el que se regula el Esquema Nacional de Seguridad) de Logicalis consiste en:

- Sistemas de Información que dan soporte al ciclo de vida completo de la gestión IT de nuestros clientes a través de nuestras organizaciones de servicios:
  - Sistemas
  - Analytics
  - Seguridad

  e incluyendo las funciones internas de negocio:
  - Comercial
  - Preventa
  - Administración
  - Recursos Humanos

Todos los sistemas/servicios descritos dentro del alcance cumplen con las medidas de seguridad de categoría **ALTA** establecidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3 Objetivos

Logicalis es responsable de desplegar los medios técnicos y humanos necesarios para garantizar el cumplimiento de las cinco dimensiones de seguridad, teniendo en cuenta los requisitos legales, reglamentarios y contractuales. En este sentido Logicalis se propone los siguientes objetivos:

- Logicalis desarrollará, implantará y mantendrá un Sistema de Gestión de la Seguridad de la Información que cumpla plenamente y, en su caso, cuente con la certificación independiente de la norma ISO 27001 para Sistemas de Gestión de la Seguridad de la Información y con el Esquema Nacional de Seguridad.
- Se identificarán y documentarán todos los activos (información, software, equipos de procesamiento electrónico de la información, utilidades de servicio y personas). Se identificarán los propietarios de todos los activos, que serán responsables del mantenimiento y la protección de sus activos.
- Todos los activos de información se clasificarán de acuerdo con sus requisitos legales y contractuales, su valor comercial, su criticidad y su sensibilidad, y la clasificación indicará los requisitos de manejo adecuados. Todos los activos de información tendrán un calendario de retención y eliminación definido.
- Deben tomarse medidas para aplicar los controles de seguridad de la información adecuados en función del valor de los activos de información y de los riesgos asociados.
- Logicalis implementará y la Dirección establecerá un proceso de evaluación de riesgos de seguridad de la información que evalúe el daño empresarial que puede resultar de un fallo de seguridad y la probabilidad realista de que dicho fallo ocurra a la luz de las amenazas y vulnerabilidades existentes, y de los controles implementados actualmente.
- Logicalis desarrollará y aplicará un plan de continuidad del negocio para contrarrestar las interrupciones de las actividades empresariales y diseñadas para proteger los procesos críticos del negocio de los efectos de fallos o desastres importantes.
- El acceso a toda la información estará controlado y se regirá por las necesidades de la empresa. Se concederá el acceso, o se adoptarán medidas para los usuarios en función de su función y de la clasificación de la información, sólo hasta un nivel que les permita desempeñar sus funciones.
- La Dirección, además, se compromete a la implantación, mantenimiento y mejora del sistema de gestión de la seguridad dotándolo de aquellos medios y recursos que sean necesarios e instando a todo el personal para que asuma este compromiso y en este sentido formará a todos sus empleados para que puedan identificar y cumplir las responsabilidades contractuales, legislativas y de seguridad de la información específicas de la empresa.
- Todas las violaciones de la seguridad de la información, reales o presuntas deberán ser notificadas e investigadas.
- Logicalis asignará la responsabilidad de la gestión del cumplimiento de la seguridad de la información a una persona o equipo que se encargue de supervisar y garantizar que las unidades organizativas operen de forma coherente con la Política de Seguridad de la Información de Logicalis y el Sistema de Gestión de la Seguridad de la Información asociado.
- Se aplicarán procesos para gestionar y mitigar los riesgos de seguridad de la información al establecer relaciones con los proveedores. La actividad de los proveedores se supervisará y auditará en función del valor de los activos y los riesgos asociados.
- Logicalis cumplirá todos los requisitos empresariales, legales y reglamentarios, así como las obligaciones contractuales.

- Logicalis impulsará un proceso de mejora continua en la gestión de la seguridad de la información, de la eficiencia y de la eficacia de la gestión de los procesos. Igualmente, la Dirección se compromete a la implantación, mantenimiento y mejora continua del SGSI dotándolo de aquellos medios y recursos que sean necesarios e instando a todo el personal para que asuma este compromiso.

La Seguridad de la Información es un esfuerzo conjunto. Requiere la implicación y participación de todos los miembros de la organización que se encuentren afectados por el alcance de la norma y más concretamente el departamento de sistemas de la organización para el desempeño de su trabajo. Por ello, cada empleado debe cumplir los requerimientos de la Política de Seguridad de la Información y su documentación asociada. Los empleados que deliberadamente o por negligencia incumplan la Política de Seguridad estarán sujetos a acciones disciplinarias según se contempla en el último capítulo de esta política.

4 Marco legal y regulatorio

Para cumplir con los objetivos referenciados en el primer punto de la presente política será necesario cumplir con requisitos legales aplicables. Por ello, hay que tener en cuenta el marco regulatorio recogido en el documento ***Cumplimiento de los requisitos legales y contractuales.***

Además, será preciso cumplir con otros requisitos que pudieran ser suscritos, *así como* los acuerdos convenidos con los clientes y la actualización continua de los mismos.

5 Datos de carácter personal

Logicalis tratará los datos personales de acuerdo con la legislación vigente y aplicable, y en concreto, respecto los principios establecidos en el artículo 5 del RGPD. Además, Logicalis consciente de la importancia que tiene la privacidad de la información. *Dispone de* un entramado de políticas, procedimientos y herramientas que dan soporte al cumplimiento de cualquier requisito que pudiera surgir en este ámbito.

Se garantiza el pleno cumplimiento del Reglamento General de Protección de Datos 676/2016 (RGPD), así como la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) que son aplicables al efecto. Con este fin se dispone de medidas técnicas y organizativas apropiadas, tomando en cuenta la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que pudieran afectar a los derechos y libertades de las personas físicas.

De igual modo Logicalis tratará los datos personales de clientes dentro de los términos contractuales establecidos (Acuerdo de Tratamiento de Datos), delimitando el objeto y la duración del tratamiento, la naturaleza y los fines del tratamiento, el tipo de datos personales, las categorías de interesados y las obligaciones y derechos del responsable. Logicalis se asegurará de que cualquier empresa subcontratada con el fin de proporcionar servicios al cliente, cumple, en el marco de los términos contractuales establecidos (Acuerdo de Tratamiento de Datos), con las mismas obligaciones estipuladas entre responsable y encargado en el Acuerdo de Protección de Datos, siempre y cuando cuente con la previa autorización del responsable del tratamiento principal.

6 Datos de carácter personal

Todos los activos de Logicalis, y sobre todo los considerados críticos, están sujetos a un análisis de riesgos con el objetivo de analizar las amenazas a las que están expuestos.

La metodología de análisis de riesgos se llevará a cabo:

- De manera periódica y como mínimo una vez al año.
- Cuando se produzca un cambio que pueda tener impacto en el servicio
- Cuando se materialice un incidente grave de seguridad o sean detectadas vulnerabilidades graves.

El Responsable de la Seguridad será el encargado de coordinar la realización de análisis de riesgos, así como de identificar las carencias y debilidades poniéndolas en conocimiento del Comité de Seguridad de la Información. El Comité de Seguridad de la Información activará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas.

Los análisis de riesgos se realizarán teniendo en cuenta los estándares de la industria.

7 Roles de seguridad

Se describen a continuación los roles y responsabilidades principales, en lo referente a aspectos de seguridad de la información de acuerdo con lo establecido en el Esquema Nacional de la Seguridad.

Las listas de tareas concretas no pretenden tener un carácter exhaustivo, pudiendo existir otras alineadas con el nivel jerárquico descrito. Estas serán, en cualquier caso, enunciativas y no limitativas de las que en cualquier momento pudieran ser exigibles por derivarse de necesidades de la empresa.

El proceso que se llevará a cabo para designar los distintos roles o puestos que tengan la función de velar por la seguridad de la información, tendrá en cuenta en todos los casos la formación de cada empleado junto a su experiencia en el puesto de trabajo, al igual que sus capacidades y aptitudes. El superior jerárquico junto al departamento de Recursos Humanos, será el encargado de valorar tales requisitos.

7.1. Responsable de la Seguridad de la Información

Encargado de determinar y aprobar qué medidas de seguridad serán aplicadas en cada sistema o subsistema, evaluando cuales son los puntos más críticos y estableciendo una serie de acciones técnicas y organizativas.

De manera más concreta, en materia de Seguridad de la Información sus funciones son las siguientes:

- Mantener la seguridad de los servicios prestado por los sistemas de la Información.
- Efectuar periódicamente análisis de riegos de los sistemas de la organización.
- Efectuar periódicamente auditorias que permitan obtener la información necesaria para cumplir con las obligaciones en materia de seguridad.
- Concienciar e informar dentro de su ámbito de responsabilidad acerca de la Seguridad de la Información.
- Comprobar que las medidas de seguridad impuestas son apropiadas para proteger la información.

- Comprobar los estados de seguridad de los sistemas y los informes de monitorización.
- Supervisar todas las incidencias de seguridad producidas desde su notificación hasta su resolución y apoyar en el supuesto que fuera necesario.
- Supervisar toda la documentación relacionada con la Seguridad de los Sistemas.
- Realizar informes de seguridad periódicamente para emitírselo al Comité de Seguridad.

Los requisitos que se tendrán en cuenta a la hora de seleccionar a la persona que cubra este puesto de trabajo serán:

- Tener titulación de ingeniería técnica.
- Será valorable experiencia en ISO 27001.

7.2. Responsable de la Información

Encargado de establecer qué requisitos debe cumplir la información que se vaya a proporcionar por cualquier medio tanto electrónico como físico, a través de los servicios de LOGICALIS. Por consiguiente, tendrá la responsabilidad de determinar a qué información se podrá acceder y *su utilidad,* siempre teniendo en cuenta el código de buenas prácticas y la legislación aplicable en materia de Protección de Datos. Además, se encargará de:

- Colaborar con el Responsable de Sistemas y el Responsable de Seguridad para el correcto mantenimiento de los sistemas clasificados en el Anexo I del Esquema Nacional de Seguridad.

Los requisitos que se tendrán en cuenta a la hora de seleccionar a la persona que cubra este puesto de trabajo serán:

- Valorable titulación de ingeniería técnica
- Experiencia en coordinación de recursos para la prestación de servicios gestionados.

7.3. Responsable de los Servicios

Encargado de establecer que requisitos de seguridad serán aplicados a los servicios prestados por LOGICALIS a través de los medios electrónicos que dispone.

De manera más concreta, en materia de Seguridad de la Información según servicios, se encargará de:

- Establecer los requisitos de los servicios de las Tecnologías de la Información y la Comunicación en materia de seguridad.
- Colaborar con el Responsable de Sistemas y el Responsable de Seguridad para el correcto mantenimiento de los sistemas clasificados en el Anexo I del Esquema Nacional de Seguridad.

Los requisitos que se tendrán en cuenta a la hora de seleccionar a la persona que cubra este puesto de trabajo serán:

- Valorable titulación de ingeniería técnica
- Experiencia en coordinación de recursos para la prestación de servicios gestionados.

7.4. Responsable de los Sistemas

Encargado de supervisar el correcto funcionamiento del sistema, así como de su instalación y de sus posibles especificaciones, añadiendo todos aquellos requisitos necesarios en materia de seguridad.

De manera más concreta, en materia de Seguridad de la Información según sistemas, se encargará de:

- Definir la Política de Gestión del Sistema, constituyendo los criterios de uso.
- Determinar la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema.
- Colaborar con el Responsable de Seguridad en los cambios que deban incluirse o que puedan afectar al sistema de seguridad.
- Supervisar qué medidas de seguridad aplicarán a los proveedores externos de componentes del sistema durante todo el ciclo de vida.
- Controlar las medidas de seguridad especificas cerciorándose de que puedan integrarse correctamente en el marco general de seguridad.
- Fijar qué características son más acordes con la configuración del software y hardware para el sistema.
- Realizar un seguimiento del proceso de análisis y gestión de los riesgos que afecten al sistema.
- Colaborar en la elaboración de toda la documentación perteneciente a la seguridad del sistema.
- Investigar los incidentes de seguridad que se hayan producido en el Sistema, comunicándoselo en el supuesto de ser necesario al Responsable de Seguridad o a quien deba corresponder.
- Constituir planes de contingencia y emergencia.
- Acordar la posible suspensión de determinado servicio o del uso de cierta información en el momento en el que sea informado de algún riesgo grave de seguridad que pudiera perjudicar al sistema. Esta decisión deberá tomarse bajo el acuerdo conjunto del resto de responsables.

Los requisitos que se tendrán en cuenta a la hora de seleccionar a la persona que cubra este puesto de trabajo serán:

- Valorable titulación de ingeniería técnica.
- Experiencia en coordinación de recursos para la prestación de servicios gestionados.

7.5. Delegado de Protección de Datos

El Delegado de Protección de Datos (DPD) es la figura encargada de garantizar el correcto cumplimiento de las obligaciones emanadas de la legislación vigente y aplicable de Protección de Datos.

De manera más concreta, se encargará de:

- Informar y asesorar de las obligaciones aplicables en virtud de la legislación aplicable de protección de datos así como de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en la legislación aplicable, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas y procedimientos de la organización en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de los análisis de riesgos y evaluaciones de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con la legislación aplicable
- Ofrecer el asesoramiento que se solicite acerca de los ejercicios de derechos de conformidad con la legislación aplicable.
- Cooperar con la autoridad de control

- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento de datos, y realizar consultas, en su caso, sobre cualquier otro asunto

Los requisitos que se tendrán en cuenta a la hora de seleccionar a la persona que cubra este puesto de trabajo serán:

- Valorable titulación universitaria que acredite conocimientos especializados en el derecho.
- Experiencia en el cumplimiento y práctica en materia de protección de datos.

7.6. Comité de seguridad de la información

El Comité de Seguridad de la Información coordina la seguridad de la información en la entidad, y estará formado por el Responsable de la Seguridad (de la Información) y por representantes de otras áreas de la organización afectadas. La composición se determinará en la Política de Seguridad de la Información de la organización. Son funciones típicas del Comité de Seguridad de la Información:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Puesto que el Comité de Seguridad de la Información no es un comité técnico, deberá recabar regularmente de personal técnico, propio o externo, la información pertinente para la toma de decisiones

o asesoramiento. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas:

- Grupos de trabajo especializados, internos, externos o mixtos.
- Asesoría externa.
- Asistencia a cursos u otro tipo de eventos formativos o de intercambio de experiencias.

El Responsable de la Seguridad (del ENS) será el secretario del Comité de Seguridad de la Información, y como tal:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

8 Obligaciones del Personal

Todo el personal de Logicalis, deberá estar concienciado en materia de seguridad y protección de datos. Debido a esto Logicalis realiza de manera periódica campañas de concienciación y de formación.

En especial aquellos empleados con responsabilidad en la administración de sistemas de información contaran con la formación adecuada para el manejo seguro de los sistemas. La realización de la formación en materia de seguridad y protección de datos será obligatoria para todos los empleados.

9 Notificación de incidentes

Logicalis cuenta con un conjunto de procedimientos internos en los que se detalla cómo se deben gestionar todos los incidentes de seguridad que puedan materializarse en cumplimiento de los requisitos del Esquema Nacional de Seguridad, así como cualquier legislación que pudiera resultar aplicable.

Debido a esto Logicalis pone a disposición de los empleados un plan de comunicación en el que se establece qué comunicar, cómo comunicar y cuándo comunicar dependiendo de la notificación que sea y en concreto la que se refiere al ámbito de seguridad de la información.

10 Directrices de estructuración, gestión y acceso a la documentación

Esta Política de Seguridad se complementa con diversos procedimientos, procesos, guías, informes y registros. Es responsabilidad del Comité de Seguridad de la Información la revisión periódica y/o mantenimiento, proponiendo, en caso de ser necesario cambios o propuestas de mejora.

Todo lo que respecta a la normativa de seguridad y, en concreto, la Política de seguridad estará a disposición de los empleados de Logicalis a través de la red corporativa de Sharepoint.

11 Terceras Partes

Cuando Logicalis preste servicios a entidades de carácter público, así como cualquier otra entidad de carácter privado, y si así se requiere por los mismos, pondrá a disposición y compartirá esta Política de Seguridad.

Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad. En caso de que Logicalis contrate servicios de terceros o ceda información, se les hará participe 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.

12 Mejora Continua

La gestión de la seguridad de la información es un proceso que debe estar en constante revisión y consecuentemente, actualización. Esta actualización debe llevarse a cabo aplicando uno de los principales objetivos y compromisos de Logicalis, siendo este la mejora continua.

A través de ese compromiso, Logicalis se preocupará de implementar a través de cambios en la organización, en los sistemas, en los procesos, herramientas, roles, etc. cualquier mejora que pueda resultar eficaz y que pueda optimizar la gestión de los servicios, evitando o previniendo amenazas, vulnerabilidades, riesgos y en general, cualquier aspecto que pudiera repercutir negativamente en la seguridad de los servicios. Para ello, Logicalis cuenta con un proceso de mejora continua en el que, y a través de diversas fuentes de obtención de información, se establecen los puntos a mejorar y los recursos necesarios para el desarrollo de estos.

35036250M ALEJANDRO ZARAGOZA (R: B82832155)

Firmado digitalmente por 35036250M ALEJANDRO ZARAGOZA (R: B82832155)
Fecha: 2025.06.04 11:17:10 +02'00'