Política de Seguridad de la Información

SGSI.PR.A5.01

CMS Albiñana & Suárez de Lezo

ÍNDICE

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. APROBACIÓN Y ENTRADA EN VIGOR

La Política de Seguridad de la Información (la "**Política de Seguridad**" o la "**Política**") ha sido revisada por el Comité de Seguridad de la Información con fecha de 23 de noviembre de 2023 y aprobada por el Comité de Dirección con fecha 13 de marzo de 2024, siendo efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Esta Política será revisada por el Comité de Seguridad de la Información, al menos, de forma anual y siempre que resulte necesario conforme a lo previsto en el apartado 5.2.

2. INTRODUCCIÓN

El presente documento expone la Política de Seguridad de la Información de CMS Albiñana & Suárez de Lezo, S.L.P. (el "**Despacho**"), que comprende el conjunto de principios básicos y líneas de actuación a los que el Despacho se compromete, de acuerdo con el Estándar Internacional ISO/IEC 27001, con el fin de ofrecer las mayores garantías de seguridad.

El objetivo de la seguridad de la información es preservar la confidencialidad, integridad y disponibilidad de la información, que constituyen los tres componentes básicos de la seguridad de la información, y tiene como objetivo establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte para la mayoría de los procesos de negocio del Despacho.

La dirección del Despacho, consciente del valor de la información, está profundamente comprometida con la política descrita en este documento.

3. ALCANCE

La presente Política de Seguridad se aplicará al Despacho y vinculará a todo su personal, independientemente de la posición y función que desempeñe.

Todo el personal del Despacho, así como personal externo que colabore con el Despacho, tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

4. PRINCIPIOS Y DIRECTRICES EN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente Política responde a las recomendaciones de las mejores prácticas de Seguridad de la Información recogidas en el Estándar Internacional ISO/IEC 27001, así como al cumplimiento de la legislación vigente en materia de protección de datos personales y de las normativas que, en el ámbito de la Seguridad de la Información, puedan afectar al Despacho. Además, el Despacho establece los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse siempre presentes en cualquier actividad relacionada con el tratamiento de información:

- **Alcance estratégico**: La seguridad de la información deberá contar con el compromiso y apoyo del nivel directivo del Despacho de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas para conformar un marco de trabajo completamente coherente y eficaz.

- **Seguridad integral**: La seguridad de la información se entenderá como un proceso integral constituido por elementos técnicos, humanos, materiales y organizativos, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información deberá considerarse como parte de la operativa habitual, estando presente y aplicándose durante todo el proceso de diseño, desarrollo y mantenimiento de los sistemas de información.

- **Gestión de riesgos**: El análisis y gestión de riesgos será parte esencial del proceso de seguridad de la información. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que están expuestos y la eficacia y el coste de las medidas de seguridad.

- **Proporcionalidad**: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

- **Mejora continua**: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado.

- **Seguridad por defecto**: Los sistemas deberán configurarse de forma que garanticen un gradosuficiente de seguridad por defecto.

El Despacho considera que las funciones de Seguridad de la Información han de estar integradas en todos los niveles jerárquicos de su personal. Puesto que la Seguridad de la Información incumbe a todo el personal del Despacho, esta Política es conocida, comprendida y asumida por todos sus empleados, así como por el personal externo que colabore con el Despacho.

Para la consecución de los objetivos de esta Política, el Despacho ha establecido una estrategia preventiva de análisis sobre los riesgos que pudieran afectarle, identificándolos, implantando controles para su mitigación y estableciendo procedimientos regulares para su reevaluación.

En el transcurso de este ciclo de mejora continua, la organización mantiene la definición tanto del nivel de riesgo residual aceptado como de sus umbrales de tolerancia.

5. REQUISITOS DE SEGURIDAD

Esta Política de Seguridad se desarrollará aplicando los siguientes requisitos:

5.1. Organización e implantación del proceso de seguridad

La seguridad de la información compromete a todos los miembros del Despacho y al personal externo que colabore con este, los cuales conocerán la Política de Seguridad y la normativa asociada.

5.2. Análisis y gestión de los riesgos

Conocer los riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para el Despacho.

Todas las redes de comunicaciones, todos los sistemas de información y los activos de información afectados por esta Política de Seguridad deberán ser objeto de un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente y, al menos, una vez al año.
- Cuando cambien el sistema de información, la información manejada y/o los servicios prestados de manera significativa.
- Cuando haya cambios en los proveedores de servicios tecnológicos o digitales para el tratamiento de la información o la prestación de servicios.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

5.3. Gestión de personal

Todo el personal del Despacho relacionado con la información y los sistemas es formado e informado de sus deberes y obligaciones en materia de seguridad, esencialmente mediante los procedimientos de seguridad que en cada caso procedan y mediante la normativa de uso de los activos.

Sus actuaciones son supervisadas según los roles establecidos para verificar que se siguen los procedimientos definidos.

5.4. Contratación y adquisiciones

Todas las contrataciones y adquisiciones que supongan o requieran acceso o tratamiento de información clasificada como no pública, se realizan amparadas por un contrato que incluya cláusulas destinadas a garantizar la salvaguarda de la confidencialidad, integridad y disponibilidad de información.

En aquellos casos en los que los servicios contratados supongan acceso o tratamiento por el proveedor de datos de carácter personal se deberá incluir en el contrato el clausulado requerido para el cumplimiento del 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 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

Las empresas y personas que con motivo de contrataciones de servicios o adquisiciones de cualquier tipo accedan a información confidencial o de uso interno, deberán conocer la Política de Seguridad de la Información y las normas y procedimientos complementarios que sean de aplicación para el objeto de la contratación.

Las empresas y personas externas que accedan a la información del Despacho deberán considerar dicha información, por defecto, como confidencial. La única información que podrán considerar como no confidencial es aquella que se haya obtenido a través de los medios de difusión pública.

5.5. Integridad y actualización del sistema

En el Despacho los sistemas se evalúan de manera periódica para conocer en todo momento su estado de seguridad, tomando en consideración las especificaciones de los fabricantes, las vulnerabilidades y las actualizaciones que procedan, y gestionando de esta manera la integridad de estos.

Todos los elementos de los sistemas requieren autorización previa a su instalación.

5.6. Protección de la información almacenada y en tránsito

La información se clasifica de acuerdo con la sensibilidad requerida en su tratamiento y según los niveles de seguridad y protección exigibles.

El Despacho presta especial atención a la información almacenada o en tránsito a través de entornos inseguros. Esto incluye la información almacenada o tratada en equipos portátiles, tabletas, smartphones, dispositivos periféricos, soportes de información, así como a las comunicaciones sobre redes abiertas o con cifrado débil, donde se aplican las medidas de seguridad que garanticen que la información se trata acorde a su clasificación.

5.7. Prevención ante otros sistemas de información interconectados

El Despacho protege el perímetro de acceso a su sistema, en particular en las conexiones a través de Internet, analizando siempre los riesgos derivados de la interconexión con otros sistemas, y estableciendo las medidas que garanticen el nivel de seguridad necesario.

5.8. Registro de actividad

El Despacho registra las actividades de sus usuarios con el fin de monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello 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 y demás disposiciones que resulten de aplicación.

5.9. Incidentes de seguridad

Cualquier compromiso de la confidencialidad, integridad, disponibilidad, autenticidad o trazabilidad de la información del Despacho se considera un incidente de seguridad.

El Despacho dispone de un sistema de detección y reacción frente a los incidentes de seguridad, que son clasificados y gestionados hasta su solución recopilando las evidencias de manera que se pueda informar y aprender de los mismos para mejorar de forma continuada.

Los usuarios disponen de canales establecidos para informar de forma inmediata de cualquier incidente o anomalía detectada.

5.10. Continuidad de la actividad

El Despacho realiza las copias de seguridad que garantizan la recuperación de la información y dispone de un plan de continuidad de negocio para garantizar la continuidad de las operaciones en caso de un incidente severo.

5.11. Mejora continua del proceso de seguridad

El sistema de gestión de seguridad implantado es actualizado y mejorado de manera continua, según establecen las certificaciones del Estándar Internacional ISO/IEC 27001.

5.12. Requisitos legales

El Despacho tiene identificada la legislación que es de aplicación. El cumplimiento de la normativa legal y reglamentaria aplicable a todos los niveles, así como la voluntad de adaptarse a futuras normas y requisitos del cliente es un compromiso y una responsabilidad del Despacho.

6. CONSECUENCIAS EN CASO DE INCUMPLIMIENTO

El incumplimiento de la Política podría dar lugar a la exigencia de responsabilidad administrativa o contractual para el Despacho derivadas, según corresponda, de la infracción de la legislación o del contrato, acuerdo u otro instrumento legal aplicables.

Si el incumplimiento es atribuible a un usuario, el Despacho podrá exigir la responsabilidad correspondiente.

* * *

Esta Política fue aprobada por el Comité de Dirección el 13 de marzo de 2024