Política de Seguridad de la Información

NAO ASSET MANAGEMENT, E.S.G. SGIIC, S.A

Clasificación Público

FECHA

Viernes, 21 de septiembre de 2024

VERSION

1.0

Control del documento

ID Documento	NAO_PSI_001_Política de Seguridad de la Información_v.1.0
Revisado por	
Aprobado por	23 de diciembre de 2024

Para cambios en este documento o registro, comuníquese con el propietario del documento / registro.

Control de versiones

Fecha	Versión	Autor	Modificaciones
21/09/2024	v.1.0	X	Versión inicial

Índice

Introducción

Este documento recoge la Política de Seguridad de la Información de NAO ASSET MANAGEMENT, E.S.G. SGIIC, S.A. (en adelante, "NAO SAM"), entendida como los principios básicos de actuación y ordenación de la organización en materia de resiliencia operativa digital y seguridad de la información. Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información, quedando excluida cualquier tipo de actuación puntual o de tratamiento coyuntural.

El resto de los documentos, prácticas, decisiones y actuaciones relacionados con la Seguridad de la Información de NAO SAM estarán alineados con las directrices contenidas en esta Política General de Seguridad de la Información.

La progresiva transformación digital de nuestra sociedad, el impacto en sectores estratégicos, como el sector financiero, el nuevo escenario de la ciberseguridad y el avance de las tecnologías de la información y comunicación, producen notables cambios a nivel internacional. Asimismo, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, advirtiéndose un notable incremento de los ciberataques, tanto en volumen y frecuencia como en sofisticación, con agentes y actores con mayores capacidades técnicas y operativas; amenazas que se producen en un contexto de alta dependencia de las tecnologías de la información y de las comunicaciones en nuestra sociedad y de gran interconexión de los sistemas de información.

Objetivo

El objetivo de la presente Política de Seguridad de la Información es establecer un marco normativo en NAO SAM que permita identificar, desarrollar e implantar las medidas técnicas y organizativas necesarias para garantizar la seguridad y protección de la información, de la privacidad de las personas, la gestión efectiva y prudente del riesgo relacionado con las TIC, así como de los sistemas de TIC que dan soporte a la actividad de NAO SAM.

Difusión

El presente documento será publicado en la intranet de NAO SAM y comunicado a todo el personal de la organización.

Así mismo, se realizará la publicación de este documento, o un resumen del mismo, en la página web de NAO SAM para poder compartirlo con las partes interesadas externas de la organización.

Compromiso de la dirección

La información, en especial los datos personales de los empleados, clientes y proveedores, así como los sistemas que la soportan, constituyen activos estratégicos para NAO SAM, que debe proteger frente a amenazas tales como errores, sabotajes, terrorismo, extorsiones, espionaje industrial, violaciones de intimidad, interrupciones de servicio y desastres naturales, con el fin de garantizar la consecución de forma eficiente y eficaz de los objetivos de negocio definidos.

La Dirección se compromete a liderar y fomentar a todos los niveles la seguridad, de acuerdo con esta Política de Seguridad y los objetivos que en ella se definen.

Política

1.1. Ámbito

NAO SAM protege los recursos involucrados en la gestión del riesgo relacionado con las TIC concerniente con el normal desarrollo de sus funciones, dando cumplimiento a la legislación vigente, preservando la confidencialidad y privacidad de la información y asegurando su disponibilidad, integridad y autenticidad. Estos objetivos se trasladan también a los sistemas de información utilizados para el desarrollo de su actividad.

Es voluntad de NAO SAM establecer condiciones de confianza en el uso de los medios electrónicos y la prestación continua de sus servicios, adoptando las medidas necesarias destinadas a proteger los sistemas de información de la organización de aquellas amenazas a los que se estén expuestos, con la finalidad de garantizar la seguridad de los sistemas de información, minimizar los riesgos y consolidar así las bases para prevenir, detectar, reaccionar y recuperarse de los posibles incidentes que puedan acaecer.

La presente Política de Seguridad de la Información se aplica en todo el ámbito de actuación del NAO SAM, es decir:

- Todos los recursos, servicios y procesos de negocio que componen NAO SAM. Se aplicará a todos los sistemas de TIC que intervienen en la prestación de servicios y a todos aquellos sistemas de soporte a las diferentes funciones y responsabilidades de NAO SAM.
- A todos los usuarios, ya sean internos o externos vinculados, directa o indirectamente, a NAO SAM que hacen uso de los sistemas descritos en el punto anterior.

1.2. Objetivos de la Seguridad de la Información

Los objetivos que hay que lograr son:

- Garantizar, asegurar e implementar las medidas de seguridad adecuadas y necesarias sobre todos los recursos, procesos, funciones y servicios relacionados directa e indirectamente con usuarios internos y externos, y con clientes, proveedores, partners u otros terceros, con la finalidad de asegurar la disponibilidad, confidencialidad, integridad, autenticidad de la información, y la conformidad con la legislación aplicable.
- Garantizar la continuidad, seguridad y calidad de los servicios ofrecidos.
- Implementar y mantener los procesos de mejora continua para favorecer la eficiencia y eficacia de las medidas de seguridad de la información, evaluando periódicamente los riesgos mediante procesos de auditoría definidos para su identificación y mitigación.
- Reducir al máximo las posibilidades de que se produzcan incidentes de seguridad y minimizar el impacto de estos en caso de que se produjeran.
- Disponer de los medios necesarios para que los diferentes usuarios de los servicios y procesos de NAO SAM hagan buen uso de la información, sistemas de la información y recursos utilizados en el desarrollo de sus funciones, obligaciones y responsabilidades, así como los que no comprometan la seguridad de la información de NAO SAM.
- Alinearse con las mejores prácticas y estándares de ámbito internacional en materia de seguridad de la información y/o ciberseguridad vigentes en cada momento.
- Aplicar las medidas de seguridad adecuadas sobre la información y datos personales tratados por medios electrónicos y en soporte en papel que NAO SAM gestiona en el ámbito de sus competencias. Esta información estará regulada por el *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, así como por la *Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).*

De acuerdo con los objetivos citados, la presente Política de Seguridad de la Información busca la adopción de los siguientes principios de seguridad, garantizando:

- **Autenticidad**: propiedad consistente en que la entidad/persona es quien dice ser o bien se garantiza la fuente de la que proceden los datos.
- **Disponibilidad**: la información y sistemas de información pueden ser utilizados en los tiempos y forma requerida.
- **Confidencialidad**: a los datos y sistemas de información solamente se accederán por las personas debidamente autorizadas.
- **Integridad**: exactitud de la información y de los sistemas de información contra la alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- **Trazabilidad**: propiedad consistente en rastrear el movimiento de cualquier usuario que forme parte del sistema de gestión.
- **Legalidad**: la información se trata de acuerdo con el marco normativo.
- **Formación**: de acuerdo con el principio de seguridad integral, garantizar un adecuado nivel de concienciación y capacitación en materia de seguridad de la información a todo el personal de la organización.
- **Gestión de incidentes**: el análisis y gestión de los riesgos como parte esencial del proceso de seguridad de la organización, manteniendo el entorno controlado y minimizando los riesgos, de acuerdo con las medidas de prevención, detección, reacción y recuperación, y estableciendo protocolos para el intercambio de información relacionada con los incidentes.

1.3. Cumplimiento normativo

La presente Política de Seguridad de la Información y el resto de documentación asociada están alineadas con el ámbito jurídico actual de leyes, reglamentos y normativas que se apliquen en **NAO SAM**, respecto a cualquier alcance material o territorial.

Para más información, revisar el documento *NAO_001_Normativa de cumplimiento de requisitos legales.*

1.4. Aplicación de recursos

La Dirección de **NAO SAM** manifiesta su compromiso de garantizar, dentro de su ámbito de funciones y responsabilidades, la provisión de recursos necesarios para implementar y mantener los procesos relacionados con la seguridad de las TIC de **NAO SAM** y su mejora continua. Todo ello con el fin de conseguir los objetivos estratégicos, la difusión, consolidación y cumplimiento de la presente Política de Seguridad de la Información, así como también implementar los mecanismos de distribución y publicación adecuados con el objetivo de que esta pueda ser conocida por los diferentes usuarios afectados por ella.

1.5. Roles y responsabilidades

Todo usuario afectado por la presente Política tendrá la obligación de:

- Cumplir en todo momento con la Política de Seguridad de la Información, normas, procedimientos e instrucciones de Seguridad de la Información de NAO SAM.
- Tener un papel activo en la ciberseguridad de cualesquiera activos que sean objeto de protección dentro del ámbito de la presente Política.
- Mantener el secreto profesional y la confidencialidad respecto de la información de NAO SAM.
- Informar, de acuerdo con la correspondiente normativa, de situaciones sospechosas o anómalas, incidentes de seguridad, y no conformidades o incumplimientos de seguridad de los sistemas de información y/o activos de la organización.

La responsabilidad general de la Seguridad de la Información recae en la persona a la que se le asignen las funciones del Responsable de Seguridad.

En caso de incumplimiento de la Política de Seguridad de la Información de NAO SAM y el resto de los documentos relacionados con la misma, así como de las medidas de seguridad que se establezcan, por parte de cualquiera al que le sea de aplicación y que ponga en riesgo la seguridad de la información en cualesquiera de sus dimensiones o los procesos que afecten a las funciones empresariales sustentadas por TIC, la Dirección de NAO SAM se reserva el derecho de iniciar las acciones correspondientes según los códigos y normas internas de comportamiento y el marco legal vigente.

1.6. Control de cumplimiento

El grado de aplicación de esta política será medido periódicamente (como mínimo anualmente) mediante autoevaluaciones coordinadas por el Responsable de Seguridad y mediante auditorías internas (como mínimo anuales), así como siempre que se produzcan cambios sustanciales en los sistemas de información de NAO SAM. La aprobación de la presente política es potestad de la Dirección de NAO SAM.

1.7. Normativas de Seguridad de la Información

La presente Política de Seguridad de la información será soportada y complementada por un conjunto de documentos específicos. Estos documentos son las denominadas Normativas de Seguridad de la Información y estarán basadas en las mejores prácticas de mercado y alineadas con las necesidades específicas de NAO SAM.

1.8. Clasificación de la información

Toda información deberá ser clasificada en virtud de su importancia para la organización y debe ser tratada según dicha clasificación, acorde a lo dispuesto en *NAO_003_Clasificación de la Información*.

1.9. Control de acceso

NAO SAM implementará medidas de seguridad físicas acorde a los escenarios de riesgos con el objetivo de impedir el acceso físico no autorizado, así como un sistema de control de acceso lógico para toda información residente en los sistemas de información TIC de la Organización.

1.10. Gestión de la seguridad basada en los riesgos y análisis y gestión de los riesgos

Todos los sistemas 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, al menos cada 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 será el encargado de que se realice el análisis de riesgos, así como identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

1.11. Proveedores y terceras partes

Todas las adquisiciones relevantes de bienes o servicios o que supongan un impacto en los servicios o sistemas de NAO SAM serán sometidos a un proceso de análisis de riesgos.

Los requisitos de seguridad de la información para la mitigación de los riesgos asociados al proveedor deben acordarse con éste y quedar documentados, debiendo aplicarse lo dictado por las normativas de seguridad establecidas y que complementan esta política.

1.12. Consecuencias por incumplimiento

El incumplimiento de esta Política y las Normativas que derivan de ella será considerado como una falta grave, dando lugar a la aplicación de la normativa sobre Régimen Disciplinario sin perjuicio de otras responsabilidades a que hubiera lugar.

Todo miembro colaborador, subcontratado o consultor está obligado al cumplimiento de esta Política, cuyo incumplimiento faculta a NAO SAM a tomar las medidas internas y/o legales que considere oportunas.

1.13. Gestión de excepciones

Cualquier excepción a la presente Política de Seguridad de la Información deberá ser registrada e informada por el Responsable de Seguridad de NAO SAM. Estas excepciones serán analizadas para evaluar el riesgo que podrían introducir a la organización y, en base a la categorización de estos riesgos, deberán ser asumidos por el peticionario de la excepción junto con los responsables del negocio.

1.14. Cambio Climático

NAO SAM ha realizado el análisis de los servicios prestados por la organización, así como su operativa habitual para la prestación de los mismos no encontrando aspectos que puedan influir en el cambio climático del planeta más allá de los generados por los sistemas de climatización, emisiones de vehículos que prestan servicio a la organización y el funcionamiento de sus sistemas TIC, siempre dentro de los requisitos legales establecidos.

Se han analizado los requisitos de las partes interesadas sin hallar ninguno específicamente relacionado con el cambio climático.

En base a ambos análisis se concluye la no necesidad de aplicar medidas más allá de los requisitos legales estándar establecidos.

1.15. Aprobación y revisión

La Política General de Seguridad de la Información es aprobada formalmente por la Dirección de NAO SAM y así quedará reflejado en las correspondientes actas, estando vigente hasta que sea reemplazada por una nueva versión. Así mismo, se revisará periódicamente y siempre que se produzcan cambios significativos que lo requieran, con el fin de adaptarla a las nuevas circunstancias, técnicas y/u organizativas, evitando que quede obsoleta.

Para estos efectos, regularmente se revisará su idoneidad, oportunidad y precisión. Las modificaciones que puedan derivarse serán propuestas por el Responsable de Seguridad para su validación.

1.16. Entrada en vigor

La Política de Seguridad de la Información entrará en vigor a partir del mismo día de su aprobación por la Dirección, su posterior publicación en la Intranet de la organización y su distribución a todo afectado por la misma.

Firmado por la Dirección de NAO SAM

www.nao-sam.com