POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ANDERSEN

INFORMACIÓN PÚBLICA

Cuadro de Control

Título:	Política de Seguridad
Tipo de documento:	Política
Nombre del fichero:	PO-Política de Seguridad de la Información
Clasificación:	Público
Estado:	Aprobado
Autor:	Director de Ciberseguridad

Revisión y aprobación		
Revisado por:	CIO	22/5/2025
Aprobado por:	Managing Partner	26/05/2025

Lista de distribución	
Corporativa	Personal de ANDERSEN y partes interesadas relevantes

ÍNDICE

Contenido

1 DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 4
2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 4
2.1 ALCANCE 4
2.2 DEFINICIONES Y SIGLAS 4
2.3 OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 5
2.4 PLANIFICACIÓN 5
2.5 IMPLANTACIÓN 6
2.6 REVISIÓN 6
2.7 MEJORAS 6
2.8 RECURSOS ASIGNADOS PARA EL SGSI 6
3 GESTIÓN DEL RIESGO 7
4 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN 7
5 ORGANIZACIÓN Y RESPONSABILIDADES 8
6 APLICACIÓN DE LA POLÍTICA 8
7 FORMACIÓN Y CONCIENCIACIÓN 8
8 GESTIÓN DE LA CONTINUIDAD DE NEGOCIO 9
9 AUDITORÍA 9
10 VALIDEZ Y ACTUALIZACIÓN 9
11 SANCIONES 10
12 VIGENCIA 10
13 RATIFICACIÓN 10

1 DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La presente política tiene por objeto facilitar las directivas o directrices que deben seguirse para proteger la información de la Organización de una amplia gama de amenazas, a fin de:

- Garantizar la seguridad de las operaciones realizadas, mediante los Sistemas de Información.
- Mitigar los incidentes de Seguridad de la Información.
- Gestionar los riesgos de Seguridad de la Información.
- Asegurar el cumplimiento de los objetivos de la Organización.

ANDERSEN tiene la voluntad de conseguir que los principios de la Política de Seguridad de la Información formen parte de la cultura de la Organización, para lo cual ha implementado un Sistema de Gestión de la Seguridad de la Información con base en un estándar reconocido internacionalmente.

Todo el personal de ANDERSEN, partes interesadas relevantes y la dirección, debe conocer y cumplir esta política.

Esta Política se desarrollará mediante normativa, procedimientos, instrucciones operativas, guías, manuales y todos aquellos instrumentos organizativos considerados útiles para alcanzar sus objetivos.

2 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

2.1 ALCANCE

El alcance de la Política de Seguridad de la Información coincide con el alcance del Sistema de Gestión de Seguridad de la Información (SGSI). Con este documento se desarrollan los requisitos exigidos por la Norma ISO/IEC 27001:2022 en su apartado: 5.2 “Política”.

Esta política abarca toda la información utilizada para el desarrollo de sus actividades por las entidades que forman parte del Sistema de Gestión de Seguridad de la Información (SGSI).

2.2 DEFINICIONES Y SIGLAS

A los efectos de una correcta interpretación de la presente Política, se incluyen las siguientes definiciones:

- **Información:** datos que poseen significado, en cualquier formato o soporte. Se refiere a toda comunicación o representación de conocimiento.
- **Sistema de Información:** se refiere a un conjunto de recursos relacionados y organizados para el tratamiento de información, según determinados procedimientos, tanto informáticos como manuales.

2.3 OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El objetivo principal de la creación de esta Política de Seguridad de la Información, por parte del Responsable del Sistema de Gestión de Seguridad de la Información (SGSI), Director de Ciberseguridad y Riesgos y de la Dirección General de ANDERSEN, es garantizar a los clientes y usuarios de los servicios el acceso a la información con la calidad y el nivel de servicio que se requieren para el desempeño acordado, así como evitar serias pérdidas o alteración de la información y accesos no autorizados a la misma.

Se establece un marco para la consecución de los objetivos de seguridad de la información para la Organización. Dichos objetivos se alcanzarán a través de una serie de medidas organizativas y de normas concretas y claramente definidas.

Esta Política de Seguridad será mantenida, actualizada y adecuada a los fines de la organización.

Los principios que deben respetarse, con base en las dimensiones básicas de la seguridad, son los siguientes:

- **Confidencialidad**: propiedad por la cual únicamente puede acceder a la información gestionada por ANDERSEN quién esté autorizado para ello, previa identificación, en el momento y por los medios habilitados.

- **Integridad:** propiedad que garantiza la validez, exactitud y completitud de la información gestionada por ANDERSEN, siendo su contenido el facilitado por los afectados sin ningún tipo de manipulación y permitiendo que sea modificada únicamente por quién esté autorizado para ello.

- **Disponibilidad:** propiedad de ser accesible y utilizable en los intervalos acordados. La información gestionada por ANDERSEN es accesible y utilizable por los clientes y usuarios autorizados e identificados en todo momento, quedando garantizada su propia persistencia ante cualquier eventualidad prevista.

Adicionalmente, dado que cualquier Sistema de Gestión de la Seguridad de la Información debe cumplir con la legislación vigente, se atenderá al siguiente principio:

- **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta ANDERSEN, especialmente en materia de protección de datos personales.

2.4 PLANIFICACIÓN

Para dar cumplimiento a la declaración de la política de seguridad, se contemplan una serie de acciones centradas en la implementación, gestión y mantenimiento de un SGSI, siempre en consonancia con dicha política. Dentro de la etapa de planificación, se considera esencial llevar a cabo un análisis de los riesgos relacionados con la seguridad de la organización. A partir de

este estudio, se elabora un plan de tratamiento específico para aquellos riesgos que la organización no considera aceptables.

2.5 IMPLANTACIÓN

La implantación del SGSI es responsabilidad principal del director de Ciberseguridad y Riesgos responsable de seguridad apoyado en todo momento por resto de directores de Área y con el total apoyo de la Dirección General.

A partir de los resultados obtenidos durante la etapa de planificación, se implementan los controles necesarios en materia de seguridad, y se ponen en funcionamiento los procedimientos definidos en el SGSI, todo ello con el objetivo de cumplir con los requisitos establecidos por las normas ISO 27001.

2.6 REVISIÓN

La política de seguridad de la información y el SGSI son revisados regularmente en intervalos planificados o si ocurren cambios relevantes, con el fin de asegurar la continua idoneidad, eficacia y efectividad de la misma. De forma genérica son revisados anualmente junto con los procesos de auditoría interna del SGSI.

2.7 MEJORAS

Las posibles mejoras de la Política de Seguridad de la información y del SGSI son establecidas bien durante las fases de revisión o bien en base a aportaciones que se consideren interesantes tanto de personal de ANDERSEN como de personal externo.

Dichas mejoras son evaluadas y una vez estudiada su viabilidad, son implementadas, operadas y mantenidas.

2.8 RECURSOS ASIGNADOS PARA EL SGSI

La empresa ANDERSEN ha identificado y puesto a disposición los recursos necesarios para garantizar el establecimiento, la implementación, el mantenimiento y la mejora continua de su Sistema de Gestión de Seguridad de la Información (SGSI). Esta asignación de recursos responde a un compromiso organizacional con la eficacia del sistema y con el cumplimiento de los objetivos estratégicos y operativos de la organización.

En cuanto a los recursos humanos, la estructura directiva responsable del SGSI está compuesta principalmente por dos figuras clave: el Chief Information Officer y el Director de Ciberseguridad y Riesgos, quienes lideran y supervisan los procesos relacionados con la gestión del sistema. Estas funciones se complementan con el soporte de una consultoría externa especializada, cuya intervención proporciona una visión objetiva, así como conocimientos técnicos adicionales que fortalecen la implementación y evolución del SGSI.

En conjunto, estos recursos permiten a ANDERSEN mantener una gestión eficaz, asegurar la conformidad con los requisitos aplicables y promover la mejora continua en todas las áreas que abarca el sistema.

3 GESTIÓN DEL RIESGO

La gestión de la Seguridad de la Información en ANDERSEN está basada en el riesgo, de conformidad con la Norma internacional ISO/IEC 27001:2022.

Se articula mediante un proceso general de apreciación y tratamiento del riesgo, que potencialmente pueden afectar a la seguridad de la información de los servicios prestados, consistente en:

- **Identificar las amenazas**, que aprovecharán vulnerabilidades de los Sistemas de Información que soportan, o de los que depende, la seguridad de la información.
- **Analizar el riesgo**, con base en la consecuencia de materializarse la amenaza y de la probabilidad de ocurrencia.
- **Evaluar el riesgo,** según un nivel previamente establecido y aprobado de riesgo ampliamente aceptable, tolerable e inaceptable.
- **Tratar el riesgo** inaceptable, mediante los controles o salvaguardas adecuadas.

Dicho proceso es cíclico y debe llevarse a cabo de forma periódica, como mínimo una vez al año. Para cada riesgo identificado se asignará un propietario, pudiendo recaer múltiples responsabilidades en una misma persona o comité.

4 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Con el objetivo de contribuir a minimizar y controlar los riesgos de la Organización, se definirán una serie de objetivos reales y medibles. Dichos objetivos deberán ser medidos, al menos, semestralmente y revisados anualmente con el fin de encontrarse alineados con la estrategia de ANDERSEN.

La fijación de objetivos de seguridad de la información se realiza teniendo en cuenta las siguientes entradas:

- Informes del director de Ciberseguridad y Riesgos y del responsable del SGSI, aprobados por la Managing Partner de ANDERSEN.
- Oportunidades de mejora encontradas durante la operación del SGSI.
- Aportaciones del delegado de Protección de Datos (DPD), quien supervisa y asesora en el cumplimiento de las normativas de protección de datos, así como en la identificación y mitigación de riesgos asociados al tratamiento de datos personales.

En la fijación de objetivos, se debe tener en cuenta que los mismos deben ser medibles y alcanzables, de ahí que la planificación para su consecución deba incluir:

- Lo que se va a hacer
- Los recursos necesarios
- Quién será el responsable
- El plazo para su consecución
- Cómo se evaluarán los resultados
- Si procede, el indicador asociado a dicho objetivo

El Managing Partner, junto con el director de Ciberseguridad y Riesgos, se responsabilizará de definir los objetivos de seguridad de la información para ANDERSEN. Estos deben ser específicos y consecuentes con su Política de Seguridad de la Información, misión, visión y valores.

5 ORGANIZACIÓN Y RESPONSABILIDADES

La organización de la seguridad de la información se organiza en torno a un Sistema de Gestión se Seguridad de la Información (SGSI) y a una serie de comités y roles involucrados en el ámbito del mismo.

- El Managing Partner de ANDERSEN es la responsable de aprobar la presente política.
- El Comité de Gestión de Riesgos de la Información es responsable de revisar la presente política.
- El director de Ciberseguridad y Riesgos es el responsable de mantener la presente política.
- El delegado de Protección de Datos supervisa y asesora en el cumplimiento de las medidas implementadas.

6 APLICACIÓN DE LA POLÍTICA

ANDERSEN ha desarrollado el presente documento que contiene la Política General para la Seguridad de la Información y que ha sido aprobada por el Managing Partner y dada a conocer a todo el personal de la empresa.

7 FORMACIÓN Y CONCIENCIACIÓN

La manera más eficaz de fortalecer la seguridad consiste en ofrecer formación continua e integrarla en las tareas laborales diarias.

Los programas de capacitación incluirán cursos específicos sobre seguridad de la información, adaptados al área correspondiente y al público al que van dirigidos, según se considere oportuno. Además, se llevarán a cabo campañas de sensibilización sobre seguridad de forma periódica, dirigidas a todo el personal, utilizando los canales que se estimen más adecuados.

El director de Ciberseguridad y Riesgos debe garantizar que todo el personal involucrado en el SGSI conoce esta política, sus objetivos y procesos, a través de su divulgación, acciones formativas y acciones de concienciación. En el caso de formación en protección de datos, tendrá en cuenta los requerimientos del delegado de Protección de Datos.

También debe garantizar la distribución de los documentos que aplican a cada nivel, de acuerdo con los diferentes roles definidos en la compañía.

8 GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

ANDERSEN dispondrá los planes necesarios para la implementación del proceso de del Análisis de Impacto al Negocio (BIA) y del Plan de Continuidad del Negocio, así como la activación de este cuando sea necesario. El departamento de Tecnologías de la Información deberá generar un Plan de Continuidad del Negocio, documentando e implementando procesos y procedimientos para asegurar la continuidad tecnológica requerida por la compañía.

Todos los empleados colaborarán en la oportuna reanudación de todos los servicios críticos para ANDERSEN en caso de una contingencia grave, ayudando de estar forma a que se restablezcan la mayoría de los servicios en el mínimo tiempo posible.

9 AUDITORÍA

La Dirección General de ANDERSEN debe garantizar y verificar, mediante auditorías internas y externas, el grado de cumplimiento de las directrices de esta Política y que estas son operadas e implementadas correctamente, responsabilizándose del cumplimiento de las medidas correctivas que hayan podido determinarse con el fin de mantener la mejora continua.

10 VALIDEZ Y ACTUALIZACIÓN

Esta política es efectiva desde el momento de su publicación y se revisa como mínimo una vez al año.

El objetivo de las revisiones periódicas es adecuarla a los cambios en el contexto de la organización, con atención a las cuestiones externas e internas, analizándose las incidencias acaecidas de seguridad de la información y las No Conformidades encontradas en el SGSI. Todo ello armonizado con los resultados de los diferentes procesos de apreciación del riesgo.

Al revisar la Política, también se revisarán todas las Normas y demás documentos que la desarrollan, siguiendo un proceso de actualización periódica sujeto a los cambios relevantes que pudieran acontecer: crecimiento de la empresa y cambios organizacionales, cambios en la infraestructura, desarrollo de nuevos servicios, entre otros.

Como consecuencia se elaborará una lista de objetivos y acciones a emprender y ejecutar durante el año siguiente para garantizar la Seguridad de la Información y el buen uso de los recursos que la soportan y tratan en ANDERSEN.

11 SANCIONES

El incumplimiento de la Política de Seguridad de la Información y demás normativas y procedimientos que la desarrollen, tendrá como consecuencia la aplicación de sanciones, conforme a la magnitud y características del aspecto no cumplido, de acuerdo con la legislación laboral vigente.

12 VIGENCIA

La Política de Seguridad de la Información entrará en vigor desde el mismo día de su publicación.

13 RATIFICACIÓN

Todos los abajo firmantes asumen y aceptan plenamente el contenido de esta Política y se comprometen a aplicarla en sus respectivas áreas para conseguir el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información.

Madrid, 26 de 05 de 2025

29175499E JOSE VICENTE MOROTE (R: B46356481)
Firmado digitalmente por 29175499E JOSE VICENTE MOROTE (R: B46356481)
Fecha: 2025.05.26 20:39:08 +02'00'

José Vicente Morote
Managing Partner

Firmado por ESPINOSA MARTINEZ JOSE MIGUEL - ***2268** el día 27/05/2025 con un certificado

Miguel Espinosa
CIO

Firmado digitalmente por DELGADO MESA JONAS - 78562999J
Nombre de reconocimiento (DN): c=ES, serialNumber=IDCES-78562999J, givenName=JONAS, sn=DELGADO MESA, cn=DELGADO MESA JONAS - 78562999J
Fecha: 2025.05.27 18:29:14 +02'00'

Jonás Delgado Mesa
Director de Ciberseguridad y Riesgos