POLÍTICA DE SEGURIDAD

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ISO/IEC 27001

VERSIÓN 1.4

MODIFICACIONES		
FECHA	**APARTADO MODIFICADO**	**CAUSA DE MODIFICACIONES**
120101	---	Emisión del Manual
121024	Clasificación de la información	Añadida "Pública"
150507	-	Adaptación a la version 2013
161102	Proveedores y clientes	Auditoría Interna 2016
180219	Mejora continua	Auditoría Interna 2017
180910	Mejora continua	Modificación de AZTI-Tecnalia por AZTI

1. ÍNDICE

1. Índice 2
2. Introducción 2
3. Descripción 3

2. INTRODUCCIÓN

2.1. OBJETIVO

Establecer los principios que rigen el manejo de información en AZTI y que aseguren que esté disponible para los usuarios autorizados, se mantenga segura y se utilice para fines legítimos.

2.2. CAMPO DE APLICACIÓN

Esta Política se aplica a toda la información adquirida, almacenada y procesada por cualquier sistema de información en AZTI . Los requerimientos regulatorios o legales de muchos países (por ejemplo, la legislación de Protección de Datos) hacen referencia expresa no sólo a la información automatizada sino también a la no automatizada. Por tanto, aunque esta Políti-

ca está referida principalmente a la información automatizada, sus principios también deben ser aplicados a la información no automatizada.

Esta Política se aplica a:

- Todos los empleados fijos y temporales de AZTI.
- Todos los terceros con acceso a la información propiedad de AZTI (entre otros, becarios, estudiantes en prácticas, etc.).

Esta Política ha sido aprobada por el Director General de AZTI. Cualquier infracción sobre la misma será tratada como una falta que podría acarrear medidas disciplinarias.

2.3. NORMATIVA APLICABLE

Esta Política se basa en la Norma ISO/ IEC 27000 series.

3. DESCRIPCIÓN

3.1. RESPONSABILIDADES

Es responsabilidad de la Unidad de Recursos y Sistemas de AZTI, a través del Responsable de Seguridad, desarrollar y mantener un Sistema de Seguridad de la Información (SGSI) que garantice que la información propiedad de AZTI está protegida del acceso y tratamiento no autorizado.

Es responsabilidad de los empleados y/ o terceros con acceso respetar y mantener la confidencialidad de la información procesada en los Sistemas de AZTI, además de respetar los principios de esta Política.

La Dirección General de AZTI demuestra su compromiso expreso con la mejora continua con la Seguridad de la Información a través de la asignación de responsabilidades específicas. Además, examina la eficacia de los controles implantados y desarrolla medidas para apoyar este proceso.

Cualquier empleado y/ o tercero con acceso que tenga constancia de un incumplimiento de los requisitos de Seguridad de la Información establecidos, debe transmitirlo al Responsable de Seguridad.

3.2. CONTROL DE ACCESO A LA INFORMACIÓN

AZTI establece procedimientos para controlar el acceso a la información, identificar a los usuarios autorizados y establecer los niveles de lectura, escritura y borrado de dicha información.

3.3. CLASIFICACIÓN DE LA INFORMACIÓN

Toda la información propiedad de AZTI es clasificada de acuerdo a su sensibilidad. Se adopta la siguiente clasificación:

- **Confidencial**: la información que está restringida a personas autorizadas y/o terceros; por ejemplo, información de carácter personal, información financiera, información asociada a proyectos de I+D sujetos a acuerdos de confidencialidad, información de gestión corporativa, contratos y acuerdos con terceros.
- **Uso interno**: la información asociada a los proyectos de I+D+i y toda aquella que se puede distribuir sin restricciones, excepto la considerada confidencial.
- **Pública**: la información obtenida de medios de acceso público.

Se han implantado restricciones de acceso a las herramientas, carpetas y/o unidades de red donde reside la información **Confidencial**.

3.4. OBLIGACIONES LEGALES

Todo el software instalado en equipos de AZTI tiene la licencia correspondiente.

3.5. EVALUACIÓN DE RIESGOS

AZTI ha establecido un proceso periódico para evaluar los riesgos asociados a su información, así como planes para reducir, transferir o aceptar dichos riesgos.

Los riesgos deben son evaluados mediante la identificación de los activos de información, las amenazas asociadas a dichos activos y las vulnerabilidades de la organización ante esas amenazas. Los tratamientos de riesgo se adecuan a la clasificación interna de la información, el impacto de una infracción y el nivel de las vulnerabilidades.

3.6. SEGURIDAD FÍSICA

AZTI ha establecido procedimientos para proteger sus Sistemas de Información, tanto como sea posible, de cualquier daño físico y del acceso no autorizado. El nivel de protección es coherente con el riesgo asociado al sistema. El chequeo de la seguridad física estará a cargo del Responsable de Seguridad.

3.7. CONTROL DE ACCESO

Cuando sea necesario dar a terceros acceso a información, dicho acceso responderá a los requisitos de seguridad adecuados y el escrupuloso respeto a lo principios de esta Política.
Se han implantado medidas para garantizar la seguridad en el acceso de los usuarios y el uso de contraseñas seguras.
Los usuarios no deben compartir sus nombres de usuario y/o contraseñas.

3.8. SEGURIDAD DE RED

El acceso a los Sistemas de Información de AZTI, a través de redes locales o remotas, está restringido a usuarios autorizados para fines autorizados. Los usuarios conectados externamente son controlados para evitar el acceso no autorizado.

3.9. GESTIÓN DE LAS VULNERABILIDADES

Existen procedimientos para garantizar la aplicación adecuada y oportuna de los parches y actualizaciones de seguridad para los sistemas operativos y aplicaciones.
Se aplican medidas de protección eficaz contra malware a todos los dispositivos.

3.10. PROCEDIMIENTO ANTE CONTINGENCIAS

AZTI ha desarrollado un Plan de Continuidad de Negocio o de respuesta ante incidencias, basado en un análisis del impacto que tendría en el negocio la interrupción de la actividad. Asimismo, dispone de una política de backup documentada y que incluye indicaciones de almacenamiento entre las tres sedes.

3.11. POLÍTICAS DE PERSONAL

Todos los usuarios de los Sistemas de Información de AZTI, incluyendo clientes, proveedores, contratistas externos y terceros que puedan tener acceso ocasional, deben ser conscientes de los requisitos de seguridad de esta Política. Los empleados deben ser conscientes de que las infracciones de seguridad o el uso inadecuado de la información de AZTI podría conllevar medidas disciplinarias contra ellos.

El Responsable de Seguridad garantiza una correcta gestión y mantenimiento de los controles de seguridad cuando un empleado deja la organización. Se presta especial atención a la eliminación de los derechos de acceso y la devolución de los activos de información.

3.12. IMPLANTACIÓN

Para garantizar la exitosa implantación de esta Política de Seguridad, la Dirección General de AZTI se compromete a que todos los empleados la conozcan y cumplan con los procedimientos de seguridad paralelos.
El Responsable de Seguridad y/o el Comité de Seguridad de AZTI examinará periódicamente la eficacia de los controles de seguridad, registros de incidencias y debilidades identificadas con el fin de diseñar mejoras y revisar esta Política.

3.13. SEGURIDAD EXTERNA

El personal externo, con carácter general, no debe tener acceso a la información de AZTI. Si por motivos de negocio fuera necesario dicho acceso, será controlado por el Responsable de Seguridad. Asimismo, estarán sujetos a los contratos de servicios y acuerdos de confidencialidad que AZTI exija para el cumplimiento del servicio.

3.14. AUDITORÍAS DE SEGURIDAD

Se ha establecido un procedimiento de auditoría interna para la revisión periódica de las medidas de seguridad implantadas en AZTI.

3.15. REVISIÓN DE LA POLÍTICA

Esta Política será revisada por el Responsable de Seguridad y/o el Comité de Seguridad de AZTI una vez al año o cuando se detecten riesgos significativos.

Cualquier cambio en esta Política deberá ser autorizado por la Dirección General.

La última versión de esta Política se puede encontrar en la Intranet de AZTI.