Política de Seguridad de la Información

1. Introducción

La presente política se elabora en cumplimiento de la exigencia del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica. Siendo Acuntia, S.A.U. (en adelante, Axians) proveedor de equipamiento y servicios de tecnologías de la información para, entre otros, la Administración Pública, ha decidido implantar voluntariamente las medidas establecidas en dicho Real Decreto e incorporarlas a su Sistema de Gestión de Seguridad de la Información, certificado conforme a requisitos ISO 27001 en su versión en vigor y para el alcance detallado en el punto 2 siguiente.

Axians, para desarrollar su actividad, necesita gestionar información y hacer uso de los sistemas que la tratan, almacenan o transmiten (sistemas TIC). En consecuencia, y con el objetivo principal de proteger los intereses de la compañía y de sus clientes, en un sector tecnológico en el que cada vez se da mayor importancia a la seguridad de la información que se trata, la dirección de Axians ha decidido formalizar la necesidad de proteger su información mediante el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI). El entorno de gestión del riesgo de Axians proporciona el contexto adecuado para la identificación, evaluación y control de los riesgos asociados. El análisis de riesgos, la declaración de aplicabilidad y el plan de tratamiento del riesgo que se han definido, describen cómo se controlan estos riesgos.

Los requisitos mínimos de seguridad establecidos en el SGSI, tal y como se recogen en el artículo 11 del ENS, son los siguientes:

a) Organización e implantación del proceso de seguridad. Las responsabilidades en materia de seguridad se identifican en el punto 5 de la presente política y la misma es comunicada y de obligado cumplimiento para todo el personal dentro del alcance del SGSI

b) Análisis y gestión de los riesgos. Realizado de forma periódica y conforme a metodología recogida en la ISO/IEC 27005

c) Gestión de personal. El personal ha sido formado e informado en relación a sus obligaciones y deberes en materia de seguridad, a través de la normativa de seguridad desarrollada. La identificación del usuario permite hacer seguimiento de la actuación del mismo, en caso de ser necesario

d) Profesionalidad. El personal encargado del SGSI está cualificado para la gestión del mismo, en las diferentes fases del ciclo de vida del servicio (implantación, operación, reversión del servicio)

e) Autorización y control de los accesos. El acceso a la información está limitado y controlado, de modo que solo los usuarios autorizados puedan acceder a ella

f) Protección de las instalaciones. Se dispone de un doble control de acceso para las áreas seguras (CPD y zona COM)

g) Adquisición de productos. Para la adquisición de productos se utilizarán, siempre que sea posible, productos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición

h) Seguridad por defecto. Las funciones de operación, administración y registro serán las mínimas necesarias y accesibles solo a las personas y equipos autorizados

i) Integridad y actualización del sistema. Todo elemento hardware o software requerirá autorización previa para su instalación en el sistema. En todo momento se conocerá el estado de seguridad de los sistemas

j) Protección de la información almacenada y en tránsito. La información almacenada y en tránsito se protege y las copias de seguridad permiten su recuperación, en su caso

k) Prevención ante otros sistemas de información interconectados. El perímetro del sistema y las conexiones con el cliente se encuentran protegidos

l) Registro de actividad. Se registra la actividad de usuario mediante recolección y gestión de logs

m) Incidentes de seguridad. Los incidentes de seguridad se registran y tratan conforme a los procedimientos establecidos

n) Continuidad de la actividad. Se dispone de un plan de contingencia y disponibilidad que permite garantizar la continuidad del servicio, en caso de pérdida de los medios habituales de trabajo

o) Mejora continua del proceso de seguridad. El SGSI se actualiza y mejora de forma continua

1.1. Prevención

Axians debe evitar o prevenir, en la medida de lo posible, que la información que maneja o los servicios que presta se vean afectados por incidentes de seguridad. Para ello, Axians ha implementado las medidas mínimas de seguridad que recogen el ENS, la norma ISO 27001 y las medidas adicionales identificadas a través de la evaluación de amenazas y riesgos. Estas medidas se han definido y documentado en la Declaración de Aplicabilidad vigente.

Para garantizar el cumplimiento de la política, Axians ha establecido mecanismos adecuados para:

- Autorizar los sistemas antes de entrar en operación

- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria y
- Solicitar la revisión periódica por parte de terceros, con el fin de obtener una evaluación independiente

1.2. Detección

Dado que los servicios de gestión remota pueden verse afectados por incidencias de seguridad, desde su ralentización hasta la imposibilidad de prestación de estos, los equipos con los que se presta el servicio se monitorizan de forma constante, de modo que se pueden prever o detectar anomalías en el funcionamiento de forma previa a su ocurrencia. Se han establecido mecanismos de detección, análisis y reporte, que llegan a los responsables del servicio regularmente, cuando se produce una desviación significativa de los parámetros respecto al rango aceptable preestablecido.

1.3. Respuesta

En caso de que se detecte un incidente de seguridad, Axians:

- Ha establecido mecanismos para responder eficazmente a los incidentes de seguridad
- Ha designado un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o terceras partes
- Ha establecido mecanismos para la comunicación e información relacionada con el incidente

1.4. Recuperación

Dentro del ámbito de aplicación de la presente política se han desarrollado planes de continuidad de los sistemas de información, que incluyen las actividades a llevar a cabo para la recuperación de los servicios.

2. Alcance

Teniendo en cuenta el contexto de Axians para el SGSI, en el cual se determinan las cuestiones internas y externas de la organización, las partes interesadas que son relevantes y sus requisitos para la seguridad de la información, Axians ha establecido el siguiente Alcance:

Sistemas de la información que dan soporte a las actividades de monitorización en remoto de infraestructuras de Tecnologías de la Información de clientes en el territorio español, de acuerdo con sus Declaraciones de Aplicabilidad vigentes.

3. Misión

Axians proporciona, a través del Centro de Servicios Gestionados (CSG) ubicado en su sede de Madrid (Calle Valle la Fuenfría 3), la gestión y monitorización de infraestructuras TIC de sus clientes, entendiendo como tales a clientes tanto externos como internos, garantizando los parámetros de eficiencia y disponibilidad requeridos por estas infraestructuras.

Los servicios prestados por Axians desde su Centro de Operación Multiservicio se resumen en la siguiente ilustración:

El COM de Axians extiende el rango de servicios tradicionales y ofrece una aproximación global y focalizada. No sólo se atienden incidencias, problemas y consultas sobre fallos de las infraestructuras de comunicación, sino que también actúa como interfaz para otras actividades como: monitorización ininterrumpida, gestión de configuraciones, gestión de cambios, gestión de acuerdos de nivel de servicio, informes personalizados, etc.

En definitiva, Axians proporciona Servicios Gestionados sobre una amplia gama de áreas TIC, con un grado de cercanía tal que permite personalizaciones con alta granularidad técnica, tanto en la observabilidad y operación de los sistemas, como en la información que es correlada y agregada casi en tiempo real, suponiendo un valor diferencial para el negocio.

4. Marco normativo

La seguridad de la información se implementa de acuerdo con las directivas de la Unión Europea, la legislación española, los acuerdos contractuales con terceras empresas y otra normativa o requisitos que Axians asume, tal y como se detallan en el documento "Normativa Aplicable" publicado en la intranet, en el siguiente enlace:
https://intranet.axians.es/sites/quality/doccenter/Normativa%20aplicable/Forms/AllItems.aspx

5. Organización de la Seguridad

5.1. Comité de Seguridad

El Comité de Seguridad está formado por el Director de Servicios Corporativos, los Responsables de Seguridad de la Información Corporativo y del COM, un Responsable en Tecnología de Seguridad, el Responsable del departamento de Transformación y Sistemas Corporativos, el Gerente de Sistemas IT, la Responsable del SGI y el Director de Personas, o en quienes estos deleguen.

El Comité es responsable de:

- Distribuir la política y la normativa de seguridad, y velar por su cumplimiento por parte de los empleados
- Aprobar la normativa de seguridad de Axians
- Revisar anualmente la Política de Seguridad
- Designar roles y responsabilidades en el ámbito de seguridad de la información
- Supervisar y aprobar tareas de seguimiento del Sistema de Gestión de Seguridad de la Información
- Realizar el seguimiento y aprobación de los riesgos identificados
- La eficacia y mejora continua del Sistema de Gestión de Seguridad de la Información
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la compañía.

5.2. Responsable de Seguridad de la Información del COM

El Responsable de Seguridad de la Información del COM es el Responsable de Herramientas y Procesos de la Unidad de Negocio de Mantenimiento y tiene, entre sus funciones, las siguientes:

- Verificar que las medidas de seguridad establecidas son adecuadas y eficaces

- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema
- Apoyar y supervisar la investigación de los incidentes de seguridad, desde su notificación hasta su resolución
- Elaborar un informe periódico de seguridad, incluyendo los incidentes más relevantes del período
- Elaborar los procedimientos de seguridad, en colaboración con el Responsable de la Información y del Servicio
- Elaborar la normativa de seguridad de la compañía
- Facultad para categorizar el sistema

5.3. Responsable de la Información y del Servicio

El Responsable de la Información y del Servicio es el Director de la Unidad de Negocio de Mantenimiento. Tiene entre sus funciones las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados
- Promover la formación y concienciación del personal encargado de la información y el servicio
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoria
- Colaborar con el Responsable de Seguridad de la Información en la ejecución de sus tareas

5.4. Designación de cargos

Quedan nombrados los siguientes cargos mediante la aprobación de la siguiente política, en los términos previstos en el presente apartado:

1. Responsable de Seguridad de la Información del COM – Responsable de Herramientas y Procesos (Unidad de Negocio de Mantenimiento)
2. Responsable de la Información, del Servicio y del Sistema – Director de Unidad de Negocio Mantenimiento.

6. Datos de carácter personal

Axians realiza tratamientos en los que hace uso de datos de carácter personal, para lo que adopta las medidas de seguridad adecuadas, siguiendo las directrices de la normativa sobre protección de datos vigente. En concreto se dispone de un Documento de Seguridad donde se desarrollan dichas medidas, que puede encontrarse publicado en la Intranet.

7. Gestión de riesgos

Todos los servicios y sistemas de información, sujetos a la presente Política, han sido objeto de un análisis de riesgos en el que se han evaluado las amenazas y riesgos a los que están expuestos. Las dimensiones de seguridad tenidas en cuenta para realizar dicho análisis de riesgos son la Disponibilidad, Integridad, Autenticidad, Confidencialidad y Trazabilidad (DICAT).

Este análisis se repite al menos una vez al año y, en todo caso, cuando cambie la información manejada, cuando cambien los servicios prestados, cuando ocurra un incidente grave de seguridad o cuando se reporten vulnerabilidades graves.

El Responsable de Seguridad de la Información del COM establece la valoración de referencia para la información manejada y el servicio afectado.

El Comité de Seguridad dinamiza la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8. Desarrollo de la Política de Seguridad de la Información

Esta política se desarrolla por medio de normativa y procedimientos de seguridad tales como control de acceso, protección frente a software malicioso, instalación de aplicaciones, acceso remoto, uso de portátiles, gestión de soportes, tratamiento de información impresa, clasificación de la información, uso de activos, uso de web, copias de respaldo, tratamiento de información de carácter personal, puesto de trabajo despejado y desatendido, gestión de claves, seguridad física, relaciones con terceros y otros controles relevantes para satisfacer los objetivos del negocio, estándares internaciones y nacionales (ISO/IEC 27001 en vigor, ENS) y código de buenas prácticas en general. Esta normativa es de obligado cumplimiento para los empleados de Axians.

La normativa de seguridad está a disposición de todos los empleados en la intranet, en el siguiente enlace: https://intranet.axians.es/sites/quality/doccenter/default.aspx y dentro del mismo, en las carpetas de Seguridad de la Información.

9. Obligaciones del personal

Todos los empleados de Axians tienen la obligación de conocer y cumplir la presente Política de Seguridad de la Información y demás normativa de seguridad existente, siendo responsabilidad del Comité de Seguridad disponer de los medios necesarios para que la información llegue a los afectados.

Se llevarán a cabo acciones formativas, al menos una vez al año, para educar y concienciar a los empleados en los aspectos más relevantes de los procedimientos de seguridad.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas, en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

En caso de incumplimiento de esta política, se derivarán sanciones de acuerdo con la legislación vigente, reglamento interno de Axians y contratos laborales, bajo la responsabilidad del departamento de Personas de Axians.

10. Terceras partes

Cuando Axians preste servicios o maneje información de terceras partes, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación con otros Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Axians utilice servicios de terceros o ceda información a terceros, se les hará igualmente partícipes de esta Política de Seguridad y de la Normativa de seguridad aplicable a dichos servicios o información. Estas terceras partes quedarán sujetas 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. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte, según se requiere en los párrafos anteriores, se realizará un informe del por parte del Responsable de Seguridad del COM, que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

11. Aprobación y entrada en vigor

La presenta Política de Seguridad de la Información se aprobó inicialmente el día 3 de Julio de 2019 por parte del Director General de Axians y es reemplazada por la presente versión de fecha 15 de marzo de 2022 aprobada por el Responsable de Seguridad de la Información.

La política de seguridad se presenta y comunica en formato impreso o electrónico a todos los empleados y a terceras partes relevantes. Es mantenida por el Responsable de Seguridad Corporativa, se revisará al menos una vez al año y se adaptará, cuando sea necesario, para reflejar las necesidades de negocio.

Santiago Hernández
Responsable de Seguridad de la Información
ACUNTIA, S.A.U.