Índice

1. Introducción y Objeto

1.1. Introducción

Para la protección y uso adecuado de la información, la Universidad Alfonso X el Sabio (en adelante UAX) ha decidido implantar un Sistema de Gestión de Seguridad de la Información (en adelante SGSI) basado en la ISO 27001, el cual va a dotar a la UAX de un conjunto de políticas, normas y procedimientos que garanticen un uso adecuado de la información y de los procesos que la tratan.

Establecer una Política de Seguridad de la Información es un requisito necesario dentro del SGSI, y es considerado la pieza angular donde se van a establecer los principios, procedimientos y normas básicas para la gestión de la seguridad de la información en la UAX, con la finalidad de preservar la confidencialidad, disponibilidad, integridad y trazabilidad de la información.

Esta política está basada en las recomendaciones de buenas prácticas para garantizar la seguridad en la gestión de Sistemas de Información (Normas internaciones ISO 27001/2) así como en la legislación vigente aplicable.

1.2. Objetivo

El objetivo principal de esta política es el establecimiento de los principios y reglas básicas para la gestión de la seguridad de la información, garantizando a los usuarios la calidad de la información y el acceso a la misma para el desempeño de sus funciones, así como evitar pérdidas de información y accesos no autorizados a la misma.

Con la adopción de esta política, la UAX persigue los siguientes objetivos.

- **Preservar la confidencialidad** de la información, asegurando el acceso exclusivamente a las personas autorizadas, previa identificación, en el momento y por los medios habilitados.

- **Mantener la integridad** de la información tratada por la UAX estableciendo los mecanismos necesarios para que la información sea completa, exacta y válida.

- **Asegura la disponibilidad** de la información tratada por UAX, para que sea accesible y utilizada por los usuarios autorizados e identificados en todo momento, quedando garantizada su propia permanencia ante cualquier eventualidad.

- **Legalidad**: UAX garantizará el cumplimiento de toda legislación que le sea de aplicación. Y, en concreto, la normativa en vigor relativa al tratamiento de datos de carácter personal.

Mediante esta política, la Dirección General de la UAX asume la responsabilidad de apoyar y promover el establecimiento de las medidas organizativas, técnicas y de control necesarias para el cumplimiento de las directrices de seguridad aquí descritas.

Asimismo, todas las políticas y procedimientos incluidos en el SGSI serán revisados, aprobados e impulsados por la Dirección General de UAX. En particular, esta Política de Seguridad será mantenida, actualizada y adecuada a los fines de la organización, alineándose con el contexto de gestión de riesgos estratégica de la organización. A este efecto se revisará siempre que se produzcan cambios significativos, y al menos una vez año, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

1.3. Alcance

La Política de Seguridad de la Información es de aplicación a todos los empleados de UAX que traten y manejen información de la universidad, así como cualquier persona externa o proveedores de servicio, que realice algún tratamiento sobre la misma ya sea en las instalaciones de la universidad o fuera de ella. Todos ellos tienen la obligación de conocer y cumplir con esta Política, y la normativa de seguridad que se derive de la misma.

De igual modo, esta Política de Seguridad de la Información es de aplicación a todos los sistemas y activos de información donde se trate información de la UAX, ya sean propios de la universidad o equipos personales.

2. Principios de Seguridad de la Información

La Política de Seguridad de la Información de la UAX se basa en los siguientes principios básicos como directrices fundamentales de seguridad de la información que han de tenerse en cuenta en cualquier actividad relacionada con el tratamiento de la información.

a) **Compromiso de la organización**: La Dirección General y todo el personal de UAX deben ser consciente de la necesidad de garantizar la seguridad de los sistemas de información, y deben entender que ellos mismos son una pieza clave en el mantenimiento de la seguridad de la información.
b) **La seguridad como proceso integrado**: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando cualquier actuación que ponga en peligro este proceso.
c) **Gestión de riesgos**: El análisis y gestión de riesgos como eje fundamental del SGSI, minimizando los riesgos mediante la implantación de medidas de seguridad y estableciendo un procedimiento regular para reevaluación
d) **Proporcionalidad**: El establecimiento de medidas y controles de protección, detección y recuperación debe ser proporcional al riesgo potencial, a la criticidad y valor de la información y procesos afectados.
e) **Mejora continua**: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la evolución del riesgo y sistema de información. La seguridad de la información será atendida, revisada y auditada por personal cualificado.
f) **Seguridad por defecto**: Debe integrarse la seguridad desde el diseño de sistemas y aplicaciones de modo que se garantice la seguridad por defecto.

3. Estructura Normativa

La normativa interna de la UAX sobre Seguridad de la Información y su constante actualización se estructurará en tres niveles relacionados de forma jerárquica:

- **Política de Seguridad**. Es el primer nivel normativo y recoge los principios rectores.
- **Normas de Seguridad**. Tratan y regulan los principios recogidos en la Política de Seguridad de la Información.
- **Procedimientos de Seguridad**. Son instrucciones de carácter técnico o procedimental que se deben observar para realizar una tarea respectando la normativa de seguridad.

4. Roles y responsabilidades

4.1 Usuarios

El personal de UAX tiene la obligación de conocer y cumplir las Normas y Procedimientos de Seguridad de la Información que puedan afectar a sus funciones, así como la Política de Seguridad de la Información y la legislación vigente, los cuales estarán a disposición de todos los empleados de la UAX que necesiten conocerlos, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

En general, cualquier persona que genera información es responsable de su clasificación de acuerdo con las instrucciones de la organización. Asimismo, cualquier persona que utiliza información y los sistemas de información está obligada a gestionarlos con el cuidado necesario, así como de utilizarlos únicamente para realizar las tareas autorizadas y en cumplimiento de las normativas válidas. Esto también es aplicable al personal externo, como proveedores, que traten información de la UAX.

Es responsabilidad de cada usuario reportar inmediatamente a la unidad de Transformación y Tecnología o a su responsable superior cualquier evento de seguridad que detecte, a fin de que el mismo sea investigado y neutralizado.

4.2 Responsable Funcional

Corresponde la función de Responsable Funcional al director o, en su caso, al colaborador que este último designe responsable funcional del Sistema de Información/Aplicación dentro de su ámbito de actuación. Esta figura tiene la responsabilidad última del uso que se haga de la información que se trate dentro de su ámbito de actuación y, por tanto, de su protección.

El **responsable Funcional** es el responsable de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

Las responsabilidades relativas a seguridad de la información son las siguientes:

- Identificar los procesos críticos que soportan los Sistemas de Información/Aplicación bajo el ámbito de su actuación y realizar una clasificación de la información que se corresponda con la calidad, valor crítico, disponibilidad e importancia relativa para la organización. La clasificación marcará el nivel de riesgo y de protección, así como el nivel de acceso al Sistema de Información/Aplicación.
- Participar de manera proactiva en el análisis de riesgos de seguridad de los Sistemas de Información/Aplicaciones bajo un ámbito de actuación.
- Administrar los usuarios en el Sistema de Información/Aplicación, actividad que incluye la autorización de altas, actualización e inactivación de usuarios, su asociación a cada uno de los roles, así como una revisión anual de los usuarios activos en el Sistema de Información/Aplicación.
- Asegurar que los requerimientos de seguridad y privacidad han sido recogidos en el análisis funcional relativos a los Sistemas de Información/Aplicaciones dentro de su ámbito de actuación.
- Validar que los requerimientos de seguridad y privacidad han sido desarrollados y son acordes a los requerimientos.
- Participar en la elaboración, divulgación del Plan de Contingencia y de Continuidad del Negocio que debe ejecutarse cuando el sistema de información/aplicación no se encuentren disponibles para garantizar la continuidad en el proceso funcional y disponibilidad de la información.
- Informar y reportar los incidentes de seguridad que detecte en la información del aplicativo bajo su responsabilidad con el fin de que se realicen las actuaciones pertinentes

4.3 Product Owner

El Product Owner será designado por la Dirección Transformación Tecnológica entre aquellos colaboradores que tengan el conocimiento técnico para atender y gestionar los requerimientos funcionales que se soliciten para un determinado Sistema de Información/Aplicación.

Su principal función en relación con la seguridad de la información es salvaguardar que el desarrollo de aplicaciones se haga de forma que se garantice la seguridad de la información, sin importar si esta información es propia de la organización o cedida por terceros.

Otras responsabilidades respecto a Seguridad de la Información.

- Validar la adecuada toma de requerimientos de seguridad y privacidad, así como la implantación de los mismos.
- Definir junto con el responsable funcional los niveles de disponibilidad (RTO-RPO) y capacidad que se requieren para los Sistemas de Información/Aplicaciones bajo su

responsabilidad.

- Definir la frecuencia de copias de seguridad de la información administrada por los Sistemas de Información/Aplicaciones bajo su responsabilidad, de manera consensuada con el Responsable Funcional.
- Participar en la elaboración del Disaster Recovery y Plan de Continuidad de Negocio, así como en las pruebas que sean programadas, en los Sistemas de Información/Aplicaciones bajo su responsabilidad.
- Informar y reportar los incidentes que detecte en el Sistema de Información/Aplicativo bajo su responsabilidad con el fin de que se realicen las actuaciones pertinentes. Así como su participación en la resolución del mismo.

4.4 Responsable de Seguridad de la Información

Es el gestor del proceso de seguridad de la información y se encarga de coordinar las diferentes actividades relacionadas con la Gestión de la Seguridad de la Información y de la (Continuidad del Negocio). Las funciones del Responsable de Seguridad de la Información son:

- Centralizar la dirección de las actividades del SGSI, coordinando todas las actuaciones en materia de seguridad dentro del alcance del SGSI.
- Determinar los niveles de seguridad de los servicios.
- Notificar la presente política a todo el personal de UAX, así como de los cambios que en ella se produzcan.
- Asegurarse de que tanto los usuarios internos como externos asumen las obligaciones de confidencial en el tratamiento de la información a la que acceden, mediante acciones de capacitación continua en materia de seguridad y la inclusión de cláusulas contractuales.
- Verificar la clasificación de la información de acuerdo con el grado de sensibilidad y criticidad de la misma, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencias.
- Notificar, en coordinación con el Departamento de Talento, Cultura y Organización, a todo el personal que ingresa en la UAX sus obligaciones respecto de cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella se deriven.
- Cubrir los requerimientos de seguridad informática establecidos para la operación, administración, desarrollo y comunicación de los sistemas y recursos tecnológicos de la empresa.
- Verificar el cumplimiento de la presente Política de Seguridad de la Información en la gestión de todos los contratos con terceros, dentro del alcance del SGSI.
- Organizar y planificar las auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de la información.

4.5 Comité de Seguridad de la Información

La dirección tiene que apoyar de forma activa la seguridad dentro de su propia organización mediante ordenes claras que demuestran compromiso, asignaciones explicitas y reconocimiento de las responsabilidades de la Seguridad de la Información. El Comité de Seguridad de la Información debe realizar las siguientes funciones:

- Asegurar que las metas de la seguridad de información sean identificadas, relacionadas con las exigencias de la organización y que sean integradas en procesos relevantes.
- Formular, revisar y aprobar la política de Seguridad de la Información.
- Proveer de direcciones claras y un gran apoyo durante la gestión de iniciativas de seguridad.
- Facilitar todos los recursos necesarios para llevar a cabo la Seguridad de la Información en su organización.
- Tomar conocimiento y supervisar la gestión de incidentes de seguridad.
- Aprobar las diferentes asignaciones de roles específicos y los responsables del Sistema de Seguridad de la Información.
- Asegurar que la implementación de los diferentes controles para la Seguridad de la Información se encuentra coordinada por la propia organización.
- Promover la difusión y apoyo a la seguridad de la información dentro de la organización.
- Nombrar y apoyar la figura del Responsable de Seguridad de la Información.

4.6 Delegado de Protección de Datos

La función principal del Delegado de Protección de Datos (DPD) es velar por la el cumplimiento de la normativa en protección de datos de carácter personal, cuyas responsabilidades son las establecidas de acuerdo con 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.

Responsabilidades:

- Asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de los datos personales.
- Supervisar el cumplimiento de lo dispuesto en la normativa vigente en materia de protección de datos, incluida la asignación de responsabilidades de concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

4.7 CTTO (Chief Transformation & Technology officer)

El CTTO, Director del Área de Tecnología y Transformación, que tendrá las siguientes funciones y responsabilidades:

- Velar por el correcto desarrollo, operación y mantenimiento de todos los sistemas de información bajo su ámbito de responsabilidad durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento, velando por su seguridad.
- Velar por la correcta definición de la la tipología y sistema de gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Velar por la implantación de las medidas de seguridad que afecten a los servicios e infraestructuras de los que es responsable.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Además, puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con el Responsable Funcional, el Procuct Owner y el Responsable de Seguridad, antes de ser ejecutada.

5. Gestión del riesgo

El análisis y la gestión de riesgos es el eje fundamental del Sistema de Gestión de Seguridad de la Información de la UAX. El nivel de riesgo y de exposición ha de mantenerse dentro de unos parámetros adecuados, mediante el despliegue de las medidas técnicas, organizativas y de seguridad apropiadas y han de estar permanentemente actualizadas.

El modelo de gestión de riesgos del SGSI de UAX es un modelo basado en el ciclo de mejora continua de DEMING. Utiliza la norma ISO 31000 como marco de gestión de riesgos con unos principios y directrices generales, combinando la metodología de Magerit y Cobit, adaptadas a los escenarios de riesgo de UAX y aplicando los marcos de control establecidos en el ENS e ISO 27002.

Todos los sistemas de información que estén sujetos a esta Política deben realizar un análisis de riesgos, determinando los riesgos y exposición de los sistemas de información. El análisis se realizará de forma regular al menos una vez cada dos años, o cuando cambien los sistemas de información, los servicios prestados o cuando se detecte un incidente grave de seguridad o vulnerabilidades graves.

6. Formación y concienciación.

La formación y concienciación en materia de Seguridad de la Información para nuestros empleados es una prioridad para la UAX.

Por ello desde la UAX se establece un plan de formación y sensibilización para garantizar los conocimientos, las habilidades y las actitudes de los empleados, con el objetivo asegurar que todos conocen y saben tratar la información de manera segura, y acorde a la normativa, políticas y procedimientos establecidos por la UAX.

7. Mantenimiento, aprobación y revisión de la política

El Responsable de Seguridad de la Información es el responsable de definir y mantener la Política de Seguridad, así como las normas y procedimientos que desarrollen esa política.

La Dirección General es la responsable de la aprobación y publicación de la Política, de distribuirla a todos los empleados y terceros afectados, así como revisar y evaluar la Política de Seguridad del SGSI.

Cualquier cambio o evolución que afecte o pudiera afectar al contenido del documento de Política de y Seguridad del SGSI quedará registrado en una nueva firma del documento de aprobación. De esta forma se concreta y confirma el compromiso de estas entidades por la calidad y seguridad de la información.

Periódicamente, y en todo caso no superando el plazo de un año, se revisará la vigencia y razonabilidad de la presente política y se llevarán a cabo las mejoras, adaptaciones o modificaciones requeridas en función de los cambios organizativos, técnicos o regulatorios aplicables.

8. Distribución de la política

El documento de Política de Seguridad del SGSI será accesible a todo el personal interno desde la intranet corporativa. Cada 12 meses se distribuirá por correo electrónico a todos los empleados internos y externos subcontratados por UAX que manejen datos y recursos pertenecientes a la misma para conocimiento y conciencia de las normas de calidad y seguridad dispuestas.

Cualquier cambio sustancial en el documento será distribuido a todos los usuarios a través de una notificación formal, enviada por correo electrónico o por comunicación interna en medios accesibles a los mismos mediante un modelo de comunicación habilitada para tal efecto.

9. Sanciones

Cualquier violación premeditada o negligente de las políticas y normas de calidad y seguridad, que suponga un potencial daño, consumado o no a UAX, será sancionada de acuerdo a los mecanismos habilitados en el convenio de la Empresa y en la normativa legal, contractual y corporativa vigentes.

Las acciones disciplinarias en respuesta a los incumplimientos de la Política de Seguridad de la Información son atribución de los Responsables Funcionales junto con la Dirección General.

10. ÍNDICE DE VERSIONES

Revisión	Fecha	Apdo. Modificado	Descripción de la Modificación
0	02/12/2021	Roles y responsabilidades	Versión inicial
0	07/09/2022	Revisión de todos los apartados	Versión inicial

ELABORADO POR	PEDRO MONTERO

REVISADO POR	PEDRO MONTERO SOFIA QUEREJETA ESTHER MALAGA

APROBADO POR	Comisión de Seguridad