# SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ISO 27001

## Datos de identificación

Nombre de la buena práctica o programa realizado: Sistema de Gestión de Seguridad de la Información ISO 27001

Objetivo de la buena práctica: Mantener y mejorar la confidencialidad, integridad y disponibilidad de la información, conforme al marco legal y normativo de la institución promoviendo una cultura de la seguridad de la información.

A quién va dirigida (población beneficiaria): Alumnado, Exalumnado, Personal Docente y Administrativo

Fecha de implementación de la buena práctica: Septiembre 2022.

Área responsable del seguimiento de la buena práctica: Dirección de Gestión de la Calidad.

## Identificación y/o contextualización de la necesidad a atender

Describa cómo se desarrolló la buena práctica

¿Cuál fue la necesidad identificada?

La era digital ha avanzado a grandes pasos lo que en consecuencia detona modificaciones en las rutinas y los métodos de trabajo, por lo que muchas de las actividades sustantivas de la institución se llevan a cabo mediante sistemas informáticos, lo que genera la necesidad de contar con un Sistema de Gestión de Seguridad de la Información que proteja los activos de nuestra Institución.

¿Cómo surgió la implementación de la buena práctica?

Se estableció la documentación necesaria para el establecimiento y seguimiento del Sistema de Gestión, destacando la identificación y seguimiento de los activos (hardware, software, infraestructura e información) del proceso de “Monitoreo de Seguridad Informática” para el planteamiento de estrategias y acciones atendiendo la confidencialidad, integridad y disponibilidad de la información, se mapearon y documentaron las actividades del proceso, se establecieron indicadores de desempeño, se elaboró el manual de seguridad de la información, manual de políticas de seguridad de la información y procedimientos, y se conformó el Comité de Seguridad de la Información.

¿Cuál era el contexto institucional en el que se suscitó la necesidad de implementar dicha práctica?

La intención de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) surge de la necesidad de proteger la información de los dispositivos y/o servicios de la UAEM y

garantizar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información conforme al marco legal y normativo de la institución.

**Acciones específicas de la atención/programa/proyecto**

Describa cuáles son sus objetivos y de qué manera los lleva a cabo

Alineados con la Política de Seguridad de la Información, la UAEM ha establecido cuatro Objetivos de Seguridad de la Información en los cuales se han realizado las siguientes acciones para su cumplimiento.

1. Contar con los recursos necesarios para implementar y mantener un SGSI: Realizar una evaluación de necesidades de infraestructura y del personal para asegurar la continuidad operativa, y establecer mecanismos para el monitoreo continuo y mejora.

2. Desarrollar una Cultura en Seguridad de la Información en el personal de la UAEM: Promover la concientización en temas de seguridad de la información mediante cursos, talleres y la difusión de las políticas de seguridad.

3. Mejorar continuamente el SGSI: Realizar auditorías internas, análisis de incidentes de seguridad, implementar indicadores de medición, controles y promover la implementación de una mejora al año por cada proceso.

4. Gestionar los activos en cumplimiento con los requisitos establecidos por la UAEM: Identificar, clasificar y proteger los activos de manera acorde con los requisitos y políticas de seguridad establecidos. Implementar controles de seguridad para la gestión de la información generada dentro del SGSI, asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad.

**Población beneficiaria**

Alumnado, Exalumnado, Personal Docente y Administrativo

**Recursos**

La Dirección General de Desarrollo Institucional, a través de Dirección de Gestión de la Calidad y el Departamento del Sistema de Gestión de Seguridad de la Información implementan acciones para la gestión del Sistema de Seguridad de la Información, para ello se cuenta con una plataforma web (Plataforma del SGSI) que administra los documentos y registros del Sistema de Gestión de Seguridad de la Información.

En cuanto a los recursos financieros y de infraestructura, se cuenta con un Programa Operativo Anual que garantiza las buenas prácticas implementadas desde el Sistema de Gestión de Seguridad de la Información, así como, con las instalaciones adecuadas, equipo y materiales para el desarrollo de las actividades.

**Logros y resultados**

Durante el año 2022, la Dirección de Gestión de la Calidad en conjunto con la Dirección General de Tecnologías de Información y Comunicación llevó a cabo reuniones de trabajo con el objetivo de implementar la Norma ISO/IEC 27001:2013 para garantizar el cumplimiento de la confidencialidad, integridad y disponibilidad conforme al marco legal y normativo de la institución, dicha implementación se establece en el proceso de "Monitoreo de Seguridad Informática" derivado de la importancia de proteger la información de los dispositivos y/o servicios de la UAEM.

Respecto a los trabajos realizados, se estableció la documentación necesaria para el establecimiento y seguimiento del Sistema de Gestión tales como son los siguientes documentos:

- Manual de seguridad de la información: Describe los procesos que interactúan en el Sistema de Gestión de Seguridad de la Información (SGSI) para cumplir con los requisitos de confidencialidad, integridad y disponibilidad de seguridad de la información alineados al modelo establecido por la norma ISO 27001, así como referenciar los documentos utilizados para implementarlo, mantenerlo y controlarlo.
- Manual de políticas de seguridad de la información: Establece los controles de seguridad para la gestión de la información generada dentro del SGSI, asegurando el cumplimiento de los principios de confidencialidad, integridad y disponibilidad.
- Procedimiento de control de información documentada: Controla la emisión y distribución de los documentos que integran el SGSI; asegurando que únicamente se utilizan los documentos vigentes. Establecer los lineamientos para identificar, compilar, codificar, acceder, archivar, almacenar, conservar y disponer de los Registros del SGSI.
- Procedimiento de planeación y tratamiento de riesgos: Establece el método para elaborar una Planeación y Tratamiento de Riesgos de los activos de los procesos que genere valor a las partes interesadas de la UAEM.
- Procedimiento de acciones correctivas: Establece los requisitos para realizar acciones correctivas en la UAEM.
- Procedimiento de auditorías internas de seguridad de la información: Establece realizar Auditorías Internas de Seguridad de la Información con el objetivo de verificar que el SGSI es conforme con las disposiciones planificadas por la norma ISO 27001 y con los requisitos establecidos por la UAEM.

- Procedimiento de términos, definiciones y abreviaciones: Controla la versión vigente de términos, definiciones y abreviaciones aplicables en el SGSI para asegurar su correcta aplicación.
- Compendio de formularios del SGSI**:** Contiene todos los formularios que se utilizan dentro del SGSI.
- Control operacional de monitoreo de seguridad informática: Establece la operación detallada del Monitoreo de Seguridad Informática, identificando quienes realizan cada una de las actividades, los documentos que se requieren para su realización, los registros para evidenciar su aplicación y, los indicadores de desempeño que se generan para su evaluación.

Capacitaciones del SGSI

Para asegurar que el personal involucrado en el proceso de Monitoreo de Seguridad Informática esté plenamente informado y comprenda a fondo la planeación estratégica, así como los requisitos específicos de la norma ISO 27001, hemos implementado un programa de capacitación integral. Este programa incluye una serie de cursos de inducción enfocados en la norma, junto con talleres dedicados a la planeación estratégica y tratamiento de riesgos y la elaboración de acciones correctivas.

Durante el periodo 2022 al 2023 y conforme al Programa Anual de Capacitación del SGSI, se impartieron cursos de capacitación a 97 participantes, como a continuación se indica:

| PROGRAMA ANUAL DE CAPACITACIÓN DEL SGSI | | | |
|---|---|---|---|
| **Periodo** | **Número de cursos** | **Número de participantes** | **Logro obtenido** |
| 2022 | 4 | 23 | Se cumplió con el 100% del programa anual de capacitación del SGSI |
| 2023 | 4 | 74 | |

Desarrollo de Plataforma Web del SGSI

Con el objetivo de centralizar los recursos para la implementación y mantenimiento del SGSI, se ha desarrollado e implementado una plataforma web exclusiva. Esta plataforma sirve como repositorio unificado para los formularios empleados en la planeación estratégica y tratamiento de riesgos de seguridad de la información. Adicionalmente, facilita el reporte y análisis mensual de los indicadores de desempeño. Una de las principales ventajas de esta innovación tecnológica es la capacidad de reforzar la confidencialidad, disponibilidad e integridad de la información. Esta herramienta digital no solo mejora la eficiencia operativa, sino que también asegura la protección y el manejo adecuado de la información estratégica de la organización.

**Impacto**

Para garantizar la buena práctica, se cuenta con un procedimiento de auditorías internas de seguridad de la información, mismo que permite evaluar la conformidad del SGSI, de conformidad con el programa anual de auditorías internas de seguridad de la información. Durante el año 2023 llevamos a cabo auditorías internas, las cuales se describen a continuación:

Auditoría interna 01/2023 de seguridad de la información bajo la norma ISO/IEC 27001:2013 al SGSI. Se llevó a cabo en los días 25 y 26 de septiembre la auditoría interna número uno (01/2023) al proceso de Monitoreo de Seguridad Informática, cuyo objetivo es verificar el cumplimiento conforme con las disposiciones planificadas en la norma ISO/IEC 27001:2013, así como con los requisitos establecidos por el SGSI UAEM.

A continuación, se muestra las auditorías internas realizadas durante el período 2022-2023:

| PROGRAMA ANUAL DE AUDITORÍAS DEL SGSI | | | | |
|---|---|---|---|---|
| **Periodo** | **Número de auditoría** | **Mes** | **Alcance** | **Logro obtenido** |
| 2022 | 01/2022 | Noviembre | Proceso de Monitoreo de Seguridad Informática | Se dio cumplimiento al programa anual de auditorías internas de seguridad de la información y se solventaron las no conformidades en tiempo y forma. |
| 2023 | 01/2023 | Septiembre | Proceso de Monitoreo de Seguridad Informática | |

Asimismo, de manera anual se evalúa a través de un organismo certificador externo, auditorías externas de seguridad de la información, con el objetivo de obtener y mantener certificados de seguridad de la información, mismos que garantizan el buen funcionamiento del SGSI.

| CERTIFICACIONES OBTENIDAS | | | |
|---|---|---|---|
| **Periodo** | **Sistema de Gestión** | **Organismo de Certificación** | **Número de Procesos/Edificios Certificados** |
| 2022 | SGSI | Quality Alliance Certification | 1 proceso certificado por primera vez |
| 2023 | SGSI | Quality Alliance Certification | Mantenimiento de 1 proceso certificado |



Av. Universidad 1001 Col. Chamilpa, Cuernavaca Morelos, México, 62209, 5o. Piso Torre de Rectoría, Tel. (777) 329 70 00, Ext. 7004 secretaria.academica@uaem.mx