

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS

SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MANUAL DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

Describir 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 27001:2013*, así como referenciar los documentos utilizados para implementarlo, mantenerlo y controlarlo.

2. ALCANCE

Aplica a los Servicios de Tecnologías de Información y Comunicación en el proceso de Monitoreo de Seguridad Informática de la Universidad Autónoma del Estado de Morelos.

Realizó	Vo.Bo.	Autorizó
<hr/> <p>Mtro. Edgar Iván Sotelo Sotelo Persona Responsable del Sistema de Gestión de Seguridad de la Información</p>	<hr/> <p>Mtra. Georgina Rosales Ariza Persona Titular de la Dirección General de Desarrollo Institucional</p>	<hr/> <p>Dr. Gustavo Urquiza Beltrán Persona Titular de la Rectoría de la UAEM</p>

ÍNDICE

	Página
1. OBJETIVO	1
2. ALCANCE	1
ANTECEDENTES	3
3. REFERENCIAS	4
4. RESPONSABILIDADES	5
5. PROCEDIMIENTO	6
<i>Marco Legal y Normativo</i>	8
<i>Representante del Comité de Seguridad de la Información</i>	8
<i>Comité de Seguridad de la Información</i>	8
<i>Contexto de la UAEM</i>	9
<i>Política de Seguridad de la Información</i>	9
<i>Objetivos de Seguridad de la Información</i>	10
<i>Políticas de Seguridad de la Información</i>	10
<i>Riesgos y Oportunidades</i>	11
<i>Tratamiento de Riesgos. El</i>	11
<i>Competencias del Personal</i>	11
<i>Entradas y salidas de los procesos</i>	12
<i>Estructura Documental</i>	13
<i>Planificación</i>	14
<i>Comunicación interna y externa</i>	16
<i>Gestión de Recursos</i>	17
<i>Adquisiciones</i>	18
<i>Control Operacional</i>	19
<i>Auditorías Internas de Seguridad de la Información</i>	19
<i>Mejora Continua</i>	20
6. ACTUALIZACIONES DEL DOCUMENTO	23

ANTECEDENTES

El 25 de diciembre de 1938 se fundó el Instituto de Estudios Superiores del Estado de Morelos, para transformarse el 7 de abril de 1953 en la Universidad del Estado de Morelos, adoptando el lema “Por una humanidad culta”.

La **UAEM** es un organismo público autónomo del Estado de Morelos con plenas facultades de gestión y control presupuestal, personalidad jurídica y patrimonio propios cuyos fines son la prestación de servicios públicos de educación de los tipos medio superior y superior, de investigación, de difusión de la cultura y extensión de los servicios.

MISIÓN

La **UAEM** es una institución educativa que forma profesionales en los niveles medio superior y superior, que sean competentes para la vida y líderes académicos en investigación, desarrollo y creación. Con ello contribuye a la transformación de la sociedad.

La docencia, la investigación y la extensión se realizan con amplias perspectivas críticas, articuladas con las políticas internas y externas dentro del marco de la excelencia académica. De esta forma, la universidad se constituye en un punto de encuentro de la pluralidad de pensamientos y se asume como protagonista de una sociedad democrática en constante movimiento.

VISIÓN

Para 2023, la **UAEM** se consolida como una institución de excelencia académica, sustentable, incluyente y segura, reconocida por la calidad de sus egresados, el impacto de su investigación, la vinculación, la difusión de la cultura y la extensión de los servicios, posicionada en los niveles estatal, regional, nacional e internacional, en un mundo interconectado a través de la innovación educativa y la economía del conocimiento. La universidad se distingue como impulsora del cambio, por la transparencia y calidad de sus procesos sustantivos y adjetivos, la consolidación de sus

redes del conocimiento como el recurso de mayor valor para el logro de sus objetivos y por su respuesta a la sociedad, que equilibra el pensamiento global con el actuar localmente.

VALORES

La **UAEM** basa su quehacer académico y administrativo en el apego a valores que orientan la toma de decisiones y caracterizan la actuación de toda la comunidad universitaria; valores que constituirán la esencia del Código Ético Institucional:

Solidaridad * Eticidad * Compromiso * Honestidad

Libertad * Justicia * Responsabilidad Social

3. REFERENCIAS

- 1.- *Manual de Políticas de Seguridad de la Información (M-SGSI-02).*
- 2.- *Procedimiento de Control de Información Documentada (P-SGSI-01).*
- 3.- *Procedimiento de Planeación y Tratamiento de Riesgos (P-SGSI-02).*
- 4.- *Procedimiento de Auditorías Internas de Seguridad de la Información (P-SGSI-03).*
- 5.- *Procedimiento de Acciones Correctivas (P-SGSI-04).*
- 6.- *Procedimiento de Términos, Definiciones y Abreviaciones (P-SGSI-05).*
- 7.- *Control Operacional de Monitoreo de Seguridad Informática (CO-SGSI-01).*
- 8.- *Compendio de Formularios del Sistema de Gestión de Seguridad de la Información. (C-SGSI-01).*
- 9.- *Manual de Perfiles de Puestos.*
- 10.- *Manual de Funciones y Responsabilidades.*

4. RESPONSABILIDADES

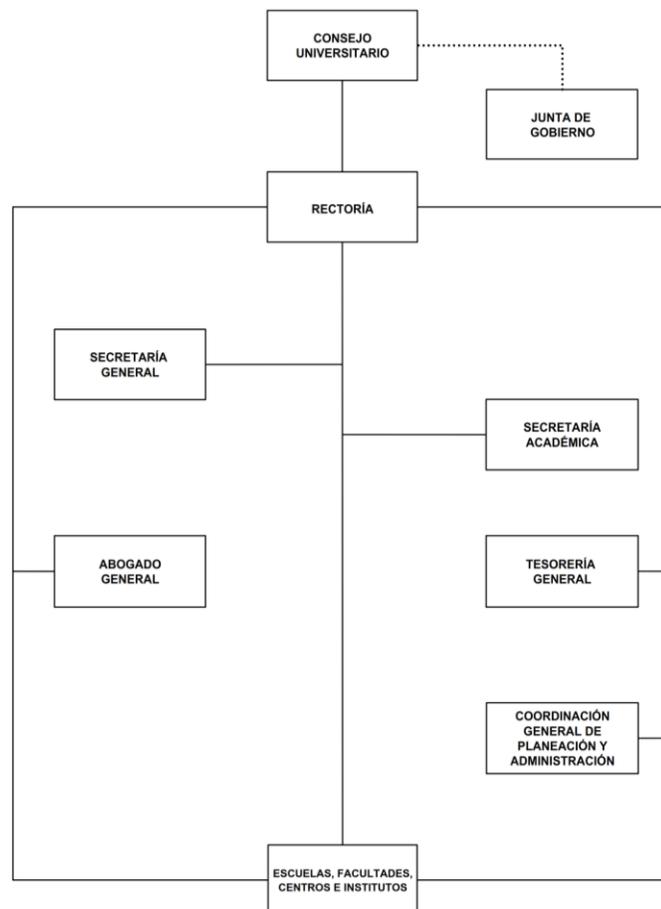
CARGO	RESPONSABILIDAD
Comité de Seguridad de la Información	<p>Integra a la Alta Dirección de la UAEM para lo relativo al SGSI.</p> <p>Establecer y mantener el <i>Contexto de la UAEM</i>, las Partes Interesadas, la <i>Política de Seguridad de la Información</i> y los <i>Objetivos de Seguridad de la Información</i> a través de la organización para aumentar la toma de conciencia, la motivación y la participación.</p> <p>Designación del Responsable del SGSI.</p> <p>Asegurarse de que se ha establecido, implementado y mantenido un SGSI eficaz y eficiente para alcanzar los <i>Objetivos de Seguridad de la Información</i>, asegurando la disponibilidad de los recursos necesarios.</p> <p>Revisar periódicamente el SGSI, así como analizar y proponer estrategias para el SGSI.</p> <p>Decidir sobre las acciones para la mejora del SGSI.</p> <p>Revisar y analizar los resultados de los <i>Objetivos de Seguridad de la Información</i> y del <i>CMI</i>.</p> <p>Analizar y aprobar el <i>Programa Anual de Capacitación</i>.</p> <p>Analizar y aprobar el <i>Programa Anual de Auditorías de Seguridad de la Información</i>.</p> <p>Analizar y proponer mejoras para los resultados de los <i>Objetivos de Seguridad de la Información</i>.</p> <p>Atender y analizar las propuestas de Mejora Continua presentadas por el personal.</p> <p>Promover el enfoque a procesos y el pensamiento basado en riesgos.</p>
Responsable del SGSI	<p>Representar al Comité de Seguridad de la Información en el SGSI, tanto dentro como fuera de la UAEM.</p> <p>Asegurarse de que se establecen, implementan y mantienen los procesos necesarios para el SGSI.</p> <p>Coordinar la revisión del Contexto de la UAEM, las Partes Interesadas y los requisitos pertinentes.</p> <p>Informar al Comité de Seguridad de la Información sobre el desempeño del SGSI y de cualquier necesidad de mejora.</p> <p>Vigilar que se implementen y difundan los documentos del SGSI.</p> <p>Reunir la información del <i>CMI</i>.</p> <p>Asegurarse de que se promueva la toma de conciencia de los requisitos de las Partes Interesadas en todos los niveles de la UAEM.</p> <p>Comunicar al personal los resultados del SGSI.</p> <p>Atender las sugerencias, comentarios o propuestas presentados por el personal.</p>
Responsable de proceso	<p>Elaborar y actualizar la identificación de activos utilizados en su proceso para su identificación, control y mantenimiento.</p> <p>Informar mensualmente los resultados obtenidos de sus procesos.</p>

	<p>Determinará los riesgos y oportunidades del Proceso. Aplicará un plan de tratamiento de riesgos con base en los activos de información del Proceso. Promoverá la toma de conciencia sobre la política, objetivos, contribución a la eficacia del SGSI y las implicaciones del incumplimiento a los requisitos.</p>
Personal	Implementar y mantener los lineamientos de este Manual.

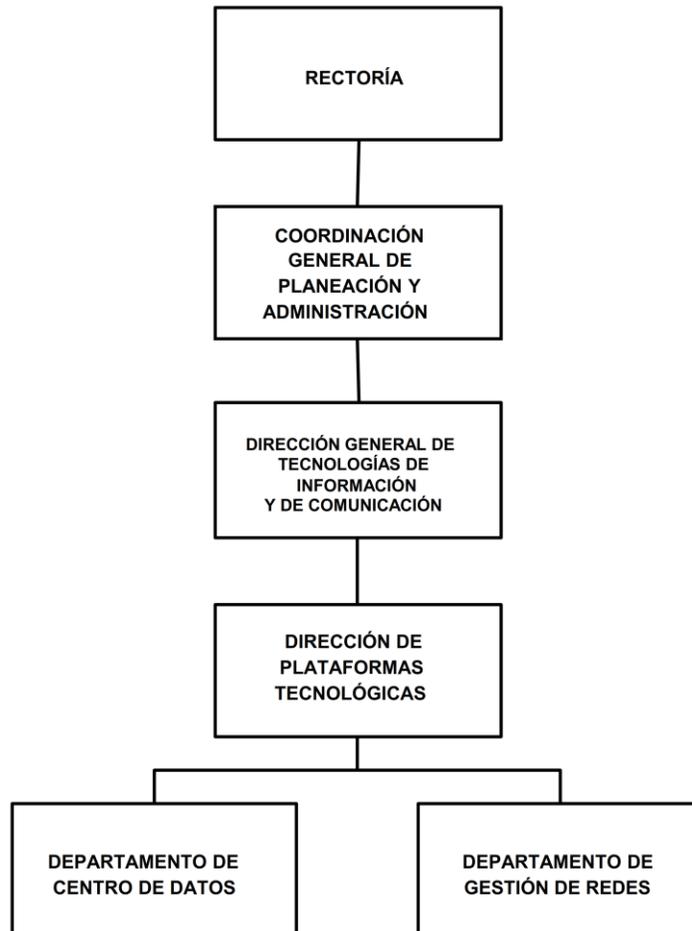
5. PROCEDIMIENTO

El personal que interviene en el **SGSI** forma parte de los siguientes organigramas en los cuales se observan los niveles de autoridad. Los roles, responsabilidades y su autoridad se detallan en el *Control Operacional* de cada proceso.

ESTRUCTURA ORGANIZACIONAL DE LA UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MORELOS



ESTRUCTURA ORGANIZACIONAL DE LA DIRECCIÓN DE PLATAFORMAS TÉCNOLÓGICAS



Marco Legal y Normativo. El **SGSI** se encuentra regulado bajo los siguientes documentos:

NOMBRE DEL PROCESO	UAEM	ESTATAL	FEDERAL
Monitoreo de Seguridad Informática.	Plan Institucional de Desarrollo 2018-2023.	Ley de Información Pública, Estadística y Protección de Datos Personales en el Estado de Morelos.	

Generales:

- 1.- Norma NMX-I-27000-NYCE-2019 *Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Fundamentos y vocabulario*
- 2.- Norma NMX-I-27001-NYCE-2015 *Tecnologías de la información - técnicas de seguridad Sistemas de gestión de seguridad de la información - Requisitos*
- 3.- Norma ISO/IEC 27001:2013 *Tecnologías de la información - técnicas de seguridad Sistemas de gestión de seguridad de la información - Requisitos*

Representante del Comité de Seguridad de la Información. El **Responsable del SGSI** es el Representante del **Comité de Seguridad de la Información**, con toda su autoridad para los asuntos relativos al **SGSI** que se detallan en este *Manual de Seguridad de la Información*. Asimismo, vigila que se difundan e implementen los documentos de Seguridad de la Información establecidos en el **SGSI**, apoyando a todo el personal involucrado por medio de reuniones de difusión, cursos y talleres, comunicados impresos y electrónicos, así como actividades de verificación.

Comité de Seguridad de la Información. La **UAEM** ha instituido un **Comité de Seguridad de la Información** conformado por:

- Persona Titular de la Rectoría de la UAEM (Persona Titular de la Presidencia del SGSI).
- Persona Titular de la Coordinación General de Planeación y Administración (Suplente de la Presidencia).
- Persona Titular de la Dirección General de Desarrollo Institucional.
- Personal Titular de la Dirección General de Tecnologías de Información y Comunicación.
- Persona Responsable del Sistema de Gestión de Seguridad de la Información (SGSI).

El **Comité de Seguridad de la Información** se reunirá de forma anual o, cuando sea necesario, a convocatoria de la **Persona Titular de la Presidencia del Comité de Seguridad de la Información**, para analizar y proponer nuevas estrategias de implementación y medición de la efectividad del **SGSI**, a través de la mejora continua. El **Comité de Seguridad de la Información**, será quién apruebe el *Programa Anual de Capacitación* y el *Programa Anual de Auditorías de Seguridad de la Información*.

Contexto de la UAEM. El Contexto de la **UAEM** y las **Partes Interesadas** serán revisados el último trimestre de cada año calendario por el **Responsable del SGSI** y el **Responsable de Proceso**, para determinar las cuestiones externas e internas que son pertinentes para su propósito y su dirección estratégica.

El **Responsable del SGSI** será quien dé seguimiento a las acciones que surjan de la revisión llevada a cabo sobre el Contexto de la **UAEM**, las **Partes Interesadas** y los requisitos pertinentes.

La **Persona Titular de la Rectoría de la UAEM** dará a conocer en su informe anual de actividades la eficacia del **SGSI**.

Política de Seguridad de la Información. La **UAEM** ha emitido su *Política de Seguridad de la Información* congruente con los propósitos organizacionales y el Contexto de la **UAEM**, con la finalidad de que sea un apoyo para el logro de su dirección estratégica. Asegurándose de que se difunda a través de pláticas, medios escritos o electrónicos, a las partes interesadas pertinentes del **SGSI**.

La *Política de Seguridad de la Información* será revisada, cuando menos, durante el último trimestre de cada año calendario por el **Comité de Seguridad de la Información** y, en caso de ser necesario, se adecuará a las expectativas de la **UAEM**; esta *Política de Seguridad de la Información* se expresa a continuación:

Política de Seguridad de la Información:

“La Universidad Autónoma del Estado de Morelos se compromete a garantizar la protección de la información de sus procesos mediante el cumplimiento de la confidencialidad, integridad y disponibilidad de la información conforme al marco legal y normativo aplicable, a través de la gestión adecuada de los activos de la Institución y el desarrollo de una cultura de seguridad de la información, fortaleciendo así la mejora continua del Sistema de Gestión, coadyuvando a mantenerse como una Universidad de Excelencia.”

Fecha de emisión: 09 de septiembre 2022

Objetivos de Seguridad de la Información. De igual manera y, alineados a la *Política de Seguridad de la Información*, la **UAEM** ha establecido cuatro *Objetivos de Seguridad de la Información* que se enuncian a continuación y que serán revisados, cuando menos, durante el último trimestre de cada año calendario por el **Comité de Seguridad de la Información**:

- 1.- Contar con los recursos necesarios para implementar y mantener un SGSI;**
- 2.- Desarrollar una Cultura en Seguridad de la Información en el personal de la UAEM;**
- 3.- Mejorar continuamente el SGSI.**
- 4.- Gestionar los activos en cumplimiento con los requisitos establecidos por la UAEM.**

Políticas de Seguridad de la Información. De igual manera y, con el objetivo de mantener la confidencialidad, integridad y disponibilidad de la información generada en el **SGSI**, estas serán revisadas, cuando menos, durante el último trimestre de cada año calendario por el **Responsable del SGSI** y el **Responsable de Proceso**.

Es función del **Responsable del SGSI** presentar al **Comité de Seguridad de la Información** los resultados obtenidos por cada uno de los *Objetivos de Seguridad de la Información*, para su análisis y propuestas de mejora.

Riesgos y Oportunidades. El **Responsable de Proceso** determinará los riesgos y oportunidades del proceso considerando el Contexto de la **UAEM** y las Partes Interesadas durante el último trimestre de cada año calendario. El **Responsable de Proceso** deberá entregar el *Cuadro de Mando Integral (F-SGSI-05)* que corresponde al proceso a su cargo durante el último trimestre de cada año calendario al **Responsable del SGSI**, donde deberán estar incluidas las estrategias y acciones para abordar los riesgos y oportunidades, a través del cual mantendrá informado de sus avances mensualmente.

Tratamiento de Riesgos. El **Responsable de Proceso** identificará los activos de información y el tratamiento de los riesgos de los mismos durante el último trimestre de cada año calendario mediante la *Identificación de Activos (F-SGSI-04a)* y *Tratamiento de Riesgos (F-SGSI-04b)*, en donde deberán estar incluidas las acciones para mitigar, transferir, aceptar o evitar los riesgos correspondientes a los activos de información del proceso.

Competencias del Personal. La educación y experiencia necesarias en cada puesto de acuerdo con el alcance del **SGSI** se describen en los siguientes documentos:

- Personal de confianza. - Manual de Perfil de Puestos de la **UAEM**.
- Personal por honorarios. - Ficha técnica y contrato de trabajo correspondiente.
- Personal administrativo sindicalizado. - Catálogo de puestos del personal administrativo sindicalizado.

En cuanto a la formación apropiada para el desempeño del puesto, el **Responsable de Proceso** determinará la formación que cada participante requiere, de conformidad con las actividades que desempeñe y la necesidad correspondiente al puesto.

A continuación, se presenta la Interacción del SGSI, el que se sustenta en la secuencia básica de Seguridad de la Información al Planear-Hacer-Verificar-Actuar (P-H-V-A), como generador de la Mejora Continua del **SGSI**:

CONTEXTO DE LA UAEM



Entradas y salidas de los procesos: Por cada proceso existen flujos diferentes, uno por cada producto generado como se detalla a continuación:

ENTRADA	PROCESO	PRODUCTO/SERVICIO (SALIDAS)
Solicitud de Monitoreo	Monitoreo de Seguridad Informática	Reporte de incidencia

Para cada proceso de los Servicios de Tecnologías de la Información y Comunicación se ha definido un *Control Operacional*, en los que se hace referencia a los documentos del sistema y se determinan los criterios o métodos que aseguran que la operación sea eficaz. Por lo que se han establecido los controles necesarios para realizar el seguimiento, medición y análisis de los procesos. De igual manera, se identifican las personas (cargos que desempeñan dentro de la **UAEM**) que realizan cada actividad del proceso o subproceso correspondiente.

En el *Control Operacional de Monitoreo de Seguridad Informática* se definen las entradas, actividades, resultados, puntos de control e información requeridos, así como documentos de referencia, cuando sea necesario, a fin de apoyar la operación y seguimiento del proceso.

Estructura Documental. El **SGSI** está conformado por una serie de documentos que describen las diferentes actividades que se realizan para mantener la Seguridad de la Información.

En la siguiente figura se muestra la estructura de la documentación:



- Manual de Seguridad de la Información:

Se refiere al documento que contiene la *Interacción del SGSI* y la referencia a toda la documentación soporte con relación al **SGSI**.

- Procedimientos Documentados:

Son los siguientes 5 documentos que se encuentran incluidos en el sistema documental del **SGSI** de la **UAEM**:

1. Control de Información Documentada.
2. Planeación y tratamiento de riesgos.
3. Auditorías Internas de Seguridad de la Información.
4. Acciones Correctivas.
5. Términos, Definiciones y Abreviaciones.

- Operación y Control de los Procesos, Control Operacional, Instrucciones de Trabajo y Formularios:

Son todos aquellos documentos propios que se utilizan para realizar los procesos y el cumplimiento de requisitos establecidos.

- Registros:

Son los documentos que presentan los resultados obtenidos o que proporcionan evidencia de las actividades desempeñadas.

Planificación. Con la finalidad de que el **Comité de Seguridad de la Información** analice de forma semestral respectivamente y, promuevan las acciones causales de los resultados esperados, en la **UAEM** se ha desarrollado un *Cuadro de Mando Integral (CMI)* identificado como formulario F-SGSI-05 y alojado en la plataforma del **SGSI**, en el que se muestra la planeación y tratamiento de riesgos para el cumplimiento de la *Política de Seguridad de la Información* y de los *Objetivos de Seguridad de la Información*, así como de todo el **SGSI**.

El *CMI* es el instrumento mediante el cual se presentan los resultados obtenidos por cada una de las cuatro perspectivas que lo conforman: Seguridad de la Información; Procesos; Formación y; Financiera, su registro será electrónico.

El formato del *CMI* se muestra a continuación:

Perspectiva de Seguridad de la Información	Perspectiva de Procesos	Perspectiva de Formación	Perspectiva Financiera
<u>Objetivo:</u>	<u>Objetivo:</u>	<u>Objetivo:</u>	<u>Objetivo:</u>
<u>Metas:</u>	<u>Metas:</u>	<u>Metas:</u>	<u>Meta:</u>
<u>Estrategia:</u>	<u>Estrategia:</u>	<u>Estrategia:</u>	<u>Estrategia:</u>
<u>Acciones a realizar:</u>	<u>Acciones a realizar:</u>	<u>Acciones a realizar:</u>	<u>Acciones a realizar:</u>
<u>Indicadores de Desempeño:</u>	<u>Indicadores de Desempeño:</u>	<u>Indicadores de Desempeño:</u>	<u>Indicadores de Desempeño:</u>

El **Responsable del SGSI** será quien reúna los resultados de los indicadores que conforman el *CMI* para informar al **Presidente del Comité de Seguridad de la Información** sobre el desempeño del **SGSI**, quien a su vez los presentará ante el **Comité de Seguridad de la Información**.

Los resultados obtenidos del **SGSI** se comunicarán semestralmente y posterior a la revisión por el **Comité de Seguridad de la Información** a todo el personal involucrado en el **SGSI** a través de una reunión informativa, en la que participará el **Responsable de Proceso** a convocatoria del **Responsable del SGSI**, utilizando como base el *CMI*, así como las acciones correctivas que se realizarán como consecuencia del análisis realizado por el **Comité de Seguridad de la Información**.

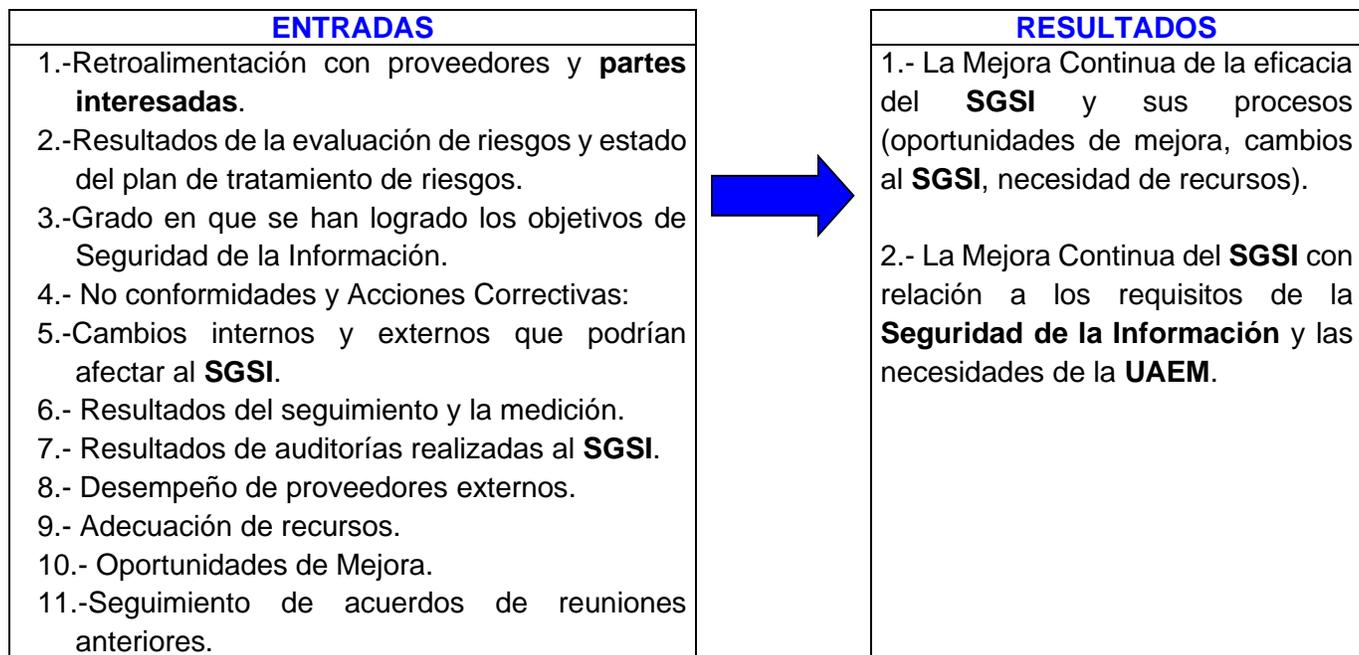
El **Responsable de Proceso** que interviene en el **SGSI**, tiene la obligación de proporcionar dentro de los primeros cinco días hábiles de cada mes los resultados obtenidos al **Responsable del SGSI**, capturando el *Informe de Indicadores Mensuales del CMI* (F-SGSI-10) en la **plataforma del SGSI**.

Comunicación interna y externa.

QUIEN COMUNICA	QUE COMUNICA	CUANDO COMUNICA	A QUIEN COMUNICAR	COMO COMUNICAR
Comité de Seguridad de la Información	eventos/cambios	Por evento	Responsable del SGSI	Documento Oficial
Responsable del SGSI	eventos/cambios	Por evento	Comité de Seguridad de la Información/Responsable de Proceso/Personal	Documento Oficial
Responsable de Proceso	eventos/cambios	Por evento	Responsable del SGSI/Personal	Documento Oficial/Verbal
Personal	eventos/cambios	Por evento	Responsable del SGSI/Responsable de Proceso/Personal	Documento Oficial/verbal
Parte Interna UAEM	eventos/cambios	Por evento	Proveedor/Institución	Documento Oficial/verbal

Referenciar al Plan de Seguridad de la Información.

A continuación, se presenta el comportamiento de la revisión del **Comité de Seguridad de la Información**:



Gestión de Recursos. A través de las reuniones de acuerdos y seguimiento del **SGSI** se identifican las necesidades de los recursos que se requieren para implementar, mantener y mejorar el **SGSI**.

En la **UAEM** se han clasificado los recursos en dos categorías:

a) **Recurso Humano:** Se han definido las competencias del personal, con base en la educación, formación y experiencias apropiadas, como se establece en el punto de competencia del personal de este manual, con relación a las actividades que afectan la Seguridad de la Información dentro del **SGSI**.

Para la selección del personal sindicalizado se aplica el *Reglamento de Admisión y Escalafón del Personal Administrativo Sindicalizado*.

En el caso de la selección de personal de confianza, el Jefe Inmediato Superior realiza las siguientes actividades de manera secuencial:

Actividad
Recepción Curricular y Evaluación Documental
Entrevista
Evaluación Técnica
Selección de Candidato para contratación
Solicitud de Contratación
Contratación (ver el proceso de movimientos y altas de personal del Sistema de Gestión de la Calidad UAEM)
Evaluación de la Competencia Laboral e Inducción

Para cada persona que participa dentro del **SGSI**, existe un expediente electrónico alojado en la **plataforma del SGSI** en el que se incluyen las evidencias del cumplimiento de la competencia laboral, a través de la *Evaluación de la Competencia Laboral* (F-SGSI-06) se actualiza y se fortalece la competencia del personal y, en caso de aplicar, incluye el programa de capacitación necesario para completar la competencia laboral requerida. Adicionalmente, el **Comité de Seguridad de la Información** programa cursos motivacionales dirigidos a todo el personal para mantener la armonía y el trabajo en equipo, necesarios para la obtención de mejores resultados y el bienestar de sus colaboradores.

Cada **Responsable de Proceso** es el encargado de actualizar las evidencias de la competencia del personal que interviene en el proceso correspondiente.

b) Infraestructura: Con la finalidad de brindar al **SGSI** con los requisitos necesarios para el cumplimiento de seguridad de la información y considerando que el área de trabajo es un punto clave para el eficiente desempeño de las funciones, así como la armonía del personal que los realiza, en la **UAEM** se ha puesto especial interés en el tema, contando en la actualidad con la infraestructura de acuerdo a las conformidades y requerimientos de las **Partes Interesadas** y de la **UAEM**, misma que se encuentra detallada en el *Inventario de Equipo*, que es elaborado y actualizado por cada **Responsable de Proceso** para su identificación, control y mantenimiento preventivo.

En el mes de junio de cada año, el **Responsable del SGSI** verificará en coordinación con cada **Responsable de Proceso** el óptimo estado y funcionamiento de la infraestructura de los bienes inmuebles, mobiliario y equipo de oficina, para gestionar el presupuesto de las acciones de mantenimiento correspondiente.

Adquisiciones. Para la adquisición o arrendamiento de bienes y servicios en la **UAEM** se aplican los siguientes Reglamentos:

- *Reglamento General de Obras y Servicios de la Universidad Autónoma del Estado de Morelos:* Tiene como objeto normar las acciones de planeación, programación, evaluación, control y en consecuencia la contratación, mantenimiento, ejecución de las obras y servicios que contrate o realice la **UAEM**.
- *Reglamento General de Adquisiciones, Arrendamientos y Servicios de la Universidad Autónoma del Estado de Morelos:* Tiene por objeto establecer las bases y procedimientos que deberán observarse para la adquisición, arrendamiento y contratación de servicios de la **UAEM**, cuyas fuentes de recursos presupuestales provengan de los erarios del Gobierno

del Estado de Morelos, de los ayuntamientos, así como de los ingresos propios y autogenerados por la **UAEM**.

Control Operacional. Los procesos del **SGSI** se realizan con base en *Controles Operacionales* que se encuentran integrados en el sistema documental del **SGSI**.

El control de información confidencial se regula conforme a lo dispuesto por la *Ley de Información Pública, Estadística y Protección de Datos Personales en el Estado de Morelos* (Incluyendo su Reglamento).

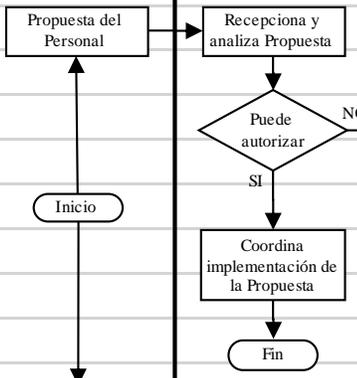
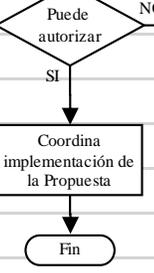
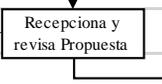
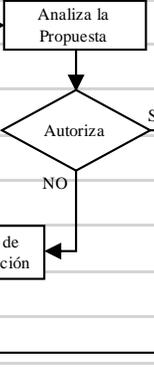
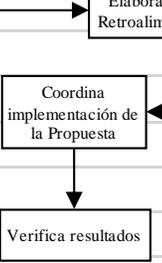
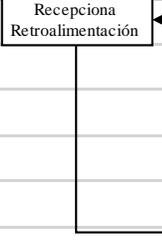
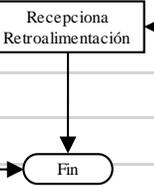
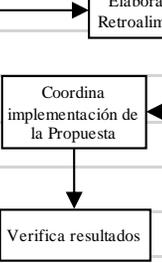
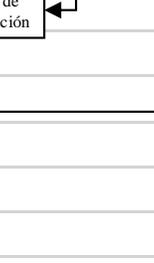
Propiedad de proveedores externos. En la operación de los Servicios de Tecnologías de Información y Comunicación no se cuenta con servicios proporcionados por **Proveedores Externos**.

Auditorías Internas de Seguridad de la Información. Con la finalidad de determinar la conformidad del **SGSI** con la norma *ISO 27001:2013* y por la organización misma, de manera eficaz, la **UAEM** contempla la planificación y realización de **Auditorías Internas de Seguridad de la Información**, mismas que son programadas y coordinadas por el **Responsable de la Gestión del Programa de Auditorías de Seguridad de la Información**. Anualmente se programan las **Auditorías Internas de Seguridad de la Información**, tomando en cuenta el estado y la importancia de los procesos, las áreas a auditar y los resultados de anteriores auditorías. (Ver procedimiento de *Auditorías Internas de Seguridad de la Información*).

Los registros generados como resultado de las actividades de auditoría son tratados de acuerdo con lo establecido en el *Procedimiento de Control de Información Documentada*.

En las reuniones del **Comité de Seguridad de la Información** se analizarán, verificarán y validarán las propuestas presentadas para corregir y/o prevenir fallas y, en su caso, serán autorizadas para su implementación, documentándose en la minuta correspondiente. Generando de esta manera, el aprendizaje organizacional y la mejora continua.

Mejora Continua. Con la finalidad de actualizar los procesos del **SGSI**, en la **UAEM** se utiliza el siguiente *Plan de la Mejora Continua*:

MEJORA CONTINUA						
PARTE INTERESADA / PERSONAL	RESPONSABLE DE PROCESO	RESPONSABLE DELSGSI	COMITÉ DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	PROCEDIMIENTO	REGISTRO	INDICADORES
					1. Escrito de propuesta.	1. # de Propuestas de Mejoras.
					1. Sugerencia, Comentario o Propuesta de la Parte Interesada	1. Propuesta.
				1. Oficina de Retroalimentación.	1. # de Acciones de Mejora.	
				1. Revisión del Responsable del SGSI.		

Las sugerencias, comentarios o propuestas por parte del personal se envían al **Responsable del SGSI** en cualquier momento, a través de la dirección de correo electrónico *sgsi@uaem.mx*, también se pueden realizar por vía telefónica o mediante un escrito en formato libre. Una vez recibidas, éstas continúan con el flujo del *Plan de Mejora Continua*.

Todas las propuestas por el personal se capturan en el módulo de mejora continua en la plataforma del **SGSI** por cada **Responsable de Proceso**, dicha propuesta debe contener:

- Objetivos de la propuesta de mejora.
- Diagrama de flujo operativo (en su caso).
- Áreas de la **UAEM** que se beneficiarán con la mejora.
- Indicadores que se utilizarán para evaluar los resultados de la mejora.

En caso de que el **Responsable de Proceso** no cuente con las facultades para autorizar la propuesta de mejora, el análisis de la propuesta será capturada en la plataforma del **SGSI** con los siguientes puntos:

- Justificación y demanda de solicitud en la mejora.
- Alineación con la *Política* y los *Objetivos de Seguridad de la Información*.
- Inversión económica requerida.
- Acciones correctivas realizadas previamente.
- Indicadores de evaluación.
- Resultados de las Auditorías de Seguridad de la Información.

Posteriormente, el **Responsable del SGSI** incluirá las propuestas de mejora en la información que será revisada y analizada por el **Comité de Seguridad de la Información** para que se realice la retroalimentación a quien hizo la sugerencia, comentario o propuesta, en el que se comunican los motivos por los cuales, en su caso, no aplica la sugerencia, comentario o propuesta después del análisis del **Comité de Seguridad de la Información**. En caso contrario y después de obtener los resultados correspondientes, se comunicarán éstos a la persona que hizo la sugerencia, comentario o propuesta. La retroalimentación se realiza a través de un oficio con formato libre cuyo

contenido es acordado por el **Comité de Seguridad de la Información** y firmado por el **Responsable del SGSI**.

Una vez que se han implementado las acciones acordadas, el **Responsable del SGSI** verifica que se hayan obtenido los resultados esperados y los comunica al **Comité de Seguridad de la Información** para en su caso, determinar las acciones pertinentes.

Para la incorporación, modificación o cancelación de un documento que se utilice en algún proceso del **SGSI**, el **Responsable de Proceso** enviará un escrito libre al **Responsable del SGSI** solicitando la autorización de la incorporación, modificación o cancelación del documento, por lo que deberá justificarlo y en su caso, anexar el nuevo documento. El **Responsable del SGSI** coordinará la actualización del *Control Operacional* correspondiente conforme al *Procedimiento de Control de Información Documentada (P-SGSI-01)*.

Para las cuestiones internas y externas que puedan afectar la integridad del **SGSI**, el **Responsable del SGSI** dará a conocer dicha información en la revisión por el **Comité de Seguridad de la Información** al **SGSI**.

6. ACTUALIZACIONES DEL DOCUMENTO

Este documento controlado ha sufrido las siguientes actualizaciones respecto a su versión anterior:

Apartado	Motivo de la actualización
Objetivo	N/A
Alcance	N/A
Referencias	N/A
Responsabilidades	N/A
Procedimiento	N/A