

MANUAL

GESTIÓN DE SEGURIDAD DE INFORMACIÓN

CÓDIGO

FECHA DE REVISIÓN

No. DE REVISIÓN

PÁGINA

MGSI-01

SEPTIEMBRE 2018

14

1 de 37

ELABORÓ

REVISÓ

APROBÓ

**REPRESENTANTE DEL SISTEMA DE
GESTIÓN DE SEGURIDAD DE
INFORMACIÓN**

RESPONSABLE DE PROCESO

ALTA DIRECCIÓN

INDICE

Contenido	Página
1. INTRODUCCION.....	4
Antecedentes de la CONSAR.....	4
Antecedentes del SGSI.....	5
Objetivos de la Seguridad de la Información.....	5
Política de Seguridad de la Información	6
2. CONSIDERACIONES.....	7
3. ALCANCE	7
4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	8
4.1 Requisitos generales.....	8
4.2 Establecimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI)	8
4.2.1 Establecimiento del SGSI.....	8
4.2.2 Implementación y operación del SGSI	9
4.2.3 Monitoreo y revisión del SGSI	9
4.2.4 Mantenimiento y mejora del SGSI.....	9
4.3 Requerimientos documentales	10
4.3.1 General	10
4.3.2 Control de documentos	11
4.3.3 Control de registros.....	12
5 RESPONSABILIDAD DE LA DIRECCIÓN.....	13
5.1 Compromiso de la Dirección.....	13
5.2 Administración de recursos.....	13
5.2.1 Provisión de recursos	13
5.2.2 Competencia, toma de conciencia y formación.....	14
6 REVISIONES INTERNAS AL SGSI.....	15
7 REVISIÓN GERENCIAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)	16

CÓDIGO	FECHA DE REVISIÓN	No. DE REVISIÓN	PÁGINA
MGSI-01	SEPTIEMBRE 2018	14	3 de 37

7.1 Generalidades	16
7.2 Entradas a la revisión	16
7.3 Resultados de la revisión	16
7.4 Proceso de Seguimiento a Revisión de la Alta Dirección	17
8 MEJORA DEL SGSI	18
8.1 Mejora continua	18
8.2 Acción correctiva	18
8.3 Acción preventiva	18
9. REFERENCIAS:	19
10. GLOSARIO DE TÉRMINOS Y DEFINICIONES	20
Anexo I	25
Medición de los indicadores del SGSI	26
DESCRIPCIÓN de los INDICADORES del SGSI	28
CONTROL DE CAMBIOS	36

1. INTRODUCCION

El presente documento tiene como finalidad establecer y dar a conocer la estructura, política, alcance y objetivos del Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de que sirva como eje rector en la operación del SGSI y coadyuve eficientemente al logro de los objetivos de seguridad de la información planteados.

Este Manual se apega y cuenta con la base legal, atribuciones, estructura orgánica y organigrama de la Comisión Nacional del Sistema de Ahorro para el Retiro.

Antecedentes de la CONSAR

Con fecha 24 de febrero de 1992 se publica en el Diario Oficial de la Federación (D.O.F.) el “Decreto que reforma, adiciona y deroga diversas disposiciones de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores” y el “Decreto que Reforma y adiciona diversas disposiciones de la Ley del Seguro Social y de la Ley del Impuesto sobre la Renta”. Asimismo, el 27 de marzo de 1992 se publica el “Decreto por el que se establece, a favor de los trabajadores al servicio de la Administración Pública Federal que estén sujetos al régimen obligatorio de la Ley del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, un Sistema de Ahorro para el Retiro”.


Posteriormente, con fecha 22 de julio de 1994, se publica la Ley para la Coordinación de los Sistemas de Ahorro para el Retiro, por la que se crea la Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR), como órgano administrativo desconcentrado de la Secretaría de Hacienda y Crédito Público, con el objeto de:

- § Establecer los mecanismos, criterios y procedimientos para el funcionamiento de los Sistemas de Ahorro para el Retiro.
- § Operar los mecanismos de protección a los intereses de los trabajadores cuentahabientes, y
- § Efectuar la inspección y vigilancia de las instituciones de crédito, de las sociedades de inversión que manejan recursos de las subcuentas de retiro y de sus sociedades operadoras, así como de cualquier otra entidad financiera que de alguna manera participe en los referidos Sistemas.

La Comisión Nacional del Sistema de Ahorro para el Retiro ha conformado su estructura administrativa para atender con eficacia y eficiencia sus atribuciones de control, inspección y vigilancia de las instituciones de crédito, de las entidades que administren sociedades de inversión, que manejen recursos de las subcuentas de retiro de las cuentas individuales y de las sociedades de inversión.

Misión: Regular y supervisar eficazmente el Sistema de Ahorro para el Retiro para que cada ahorrador construya su patrimonio pensionario.

Visión: Ser la Institución que consolide un sistema confiable e incluyente, pilar preponderante del patrimonio de los ahorradores para el retiro.

		MANUAL	
		GESTIÓN DE SEGURIDAD DE INFORMACIÓN	
CÓDIGO	FECHA DE REVISIÓN	No. DE REVISIÓN	PÁGINA
MGSI-01	SEPTIEMBRE 2018	14	5 de 37

Antecedentes del SGSI

En algunos procesos que se realizan en las actividades inherentes de la CONSAR, se identificó que implicaba el manejo de información que está clasificada como Información Restringida, y por tal motivo, se determinó instrumentar un mecanismo de control de seguridad de la información que permitiera ofrecer a todos los trabajadores inscritos en el Sistema de Retiro, la confianza y la certeza de que la información sería utilizada con los más altos controles de seguridad posibles.

Como resultado de ésta situación, en 2005, la CONSAR decidió implementar el estándar internacional en materia de Seguridad de la Información ISO 27001:2005 y obtener la Certificación que avalara que los procesos declarados en su alcance, se utilizaría con las reglas y buenas practicas que establece la Norma Internacional.

La Certificación fue obtenida y conservada durante el periodo de 2006 a 2014, año en el que fue publicado en el Diario Oficial de la Federación (DOF), las políticas y disposiciones para la Estrategia Digital Nacional, y establece con carácter vinculatorio el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información (MAAGTICSI).

Estos lineamientos que deben aplicarse, y las buenas prácticas que se adoptaron cuando se mantuvo la Certificación del ISO 27001, son la base de la seguridad de la información que rige y que deberá cumplir todo el personal de la CONSAR.

Toda referencia al estándar internacional de la norma ISO 27001:2005 citada en este Manual y demás documentos de Políticas y Procedimientos, deberá considerarse como una forma de trabajo que se adoptó y se mantiene como referencia, sin que se deba utilizar como emblema o asumir como Empresa Certificada, estableciéndose que, en cualquier documento que se elabore o modifique, deberán suprimirse las referencias a esta norma.

Descripción de Términos: Para consulta de cualquier definición en este documento o en los Procedimientos de Gestión, refiérase a la sección de Glosario de Términos y Definiciones ubicado al final de este documento.

Objetivos de la Seguridad de la Información

1. Reconocer el valor de la información como medio para fortalecer a la Comisión.
2. Garantizar la continuidad operativa de los procesos definidos en el Alcance del Sistema de Gestión de Seguridad de la Información.
3. Promover una cultura de seguridad y protección hacia los activos de información.
4. Mantener la confidencialidad, disponibilidad e integridad de la información de la Comisión.
5. Minimizar el impacto de incidentes de seguridad de información de los activos involucrados en el Alcance del Sistema de Gestión de Seguridad de la Información.

Política de Seguridad de la Información

La política de seguridad de la información ha nacido de la visión, misión y objetivos de seguridad de la información establecidos por la Alta Dirección y es considerada un soporte básico para lograr en tiempo y forma los objetivos planeados.

La política de seguridad de la información es revisada anualmente o antes si se considera necesario. Cualquier cambio es comunicado a todo el personal a través de los mecanismos de comunicación de la CONSAR.

A continuación se enuncia la política de seguridad de información de la CONSAR:

GARANTIZAR Y MANTENER LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN INVOLUCRADA EN EL PROCESO DE RECEPCIÓN DE INFORMACIÓN AGREGADA Y A DETALLE RELACIONADA A LA BASE DE DATOS NACIONAL DEL SAR, CONTROLANDO SU ACCESO Y USO ÚNICAMENTE PARA PROPÓSITOS AUTORIZADOS DENTRO DEL MARCO LEGAL Y NORMATIVO DE LA CONSAR.

REVISAR Y MEJORAR CONTINUAMENTE EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA DISMINUIR LOS NIVELES DE RIESGO ASOCIADOS A LA INFORMACIÓN Y CUMPLIR CON NUESTROS OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN ESTABLECIDOS.

		MANUAL	
		GESTIÓN DE SEGURIDAD DE INFORMACIÓN	
CÓDIGO	FECHA DE REVISIÓN	No. DE REVISIÓN	PÁGINA
MGSI-01	SEPTIEMBRE 2018	14	7 de 37

2. CONSIDERACIONES

El presente documento (Manual del Sistema de Gestión de Seguridad de la Información, MSGSI), describe como está conformado el Sistema de Gestión de Seguridad de la Información de la CONSAR.

Este documento se caracteriza por:

- Dar cumplimiento a los lineamientos establecidos por el Gobierno Federal en materia de Seguridad de la Información.
- Ser el marco de referencia para implementar el Sistema de Gestión de Seguridad de la Información.
- Describir la estructura del Sistema de Gestión de Seguridad de la Información.
- Dar a conocer las responsabilidades de las áreas involucradas y las referencias a sus documentos.

3. ALCANCE

El Sistema de Gestión de Seguridad de la Información incluye el personal, la infraestructura de servicios y la tecnología del proceso de recepción de información agregada y a detalle relacionada a la Base de Datos Nacional del SAR

Ubicadas en:

El 2° piso de las instalaciones de la Comisión con domicilio en Camino a Santa Teresa No 1040, Colonia Jardines en la Montaña, C.P. 14210, Delegación Tlalpan, Ciudad de México

4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Las revisiones al Manual del Sistema de Gestión de Seguridad de la Información se realizan cada vez que se emitan procedimientos nuevos, se adopten herramientas o controles al Sistema de Gestión de Seguridad de la Información, proceso o servicio, o como consecuencia de la implantación del proceso de mejora continua.

La información contenida en el presente manual está disponible para cualquier miembro de la Institución, auditores externos e internos, consultas por parte de nuestros usuarios y otras instituciones, y en situaciones donde se requiera conocer el Sistema de Gestión de Seguridad de la Información de la CONSAR.

4.1 Requisitos generales

La CONSAR ha establecido e implementado un Sistema de Gestión de Seguridad de la Información (SGSI), el cual es operado, monitoreado, revisado, mantenido y mejorado continuamente, lo anterior con el objetivo de alcanzar los niveles apropiados de confidencialidad, integridad y disponibilidad de la información que requiere la organización.

4.2 Establecimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI)

La Alta Dirección planifica y mantiene el SGSI, de tal manera que se asegure de cumplir con los requisitos y objetivos de seguridad de la información.

4.2.1 Establecimiento del SGSI

Como parte del establecimiento del SGSI, la CONSAR realiza las siguientes acciones:

- a) El alcance y límites del SGSI están definidos en el punto 3 de este manual.
- b) La Alta Dirección aprobó una política de seguridad de información, la cual se encuentra documentada en el punto 1 de este manual.
- c) Se tiene definida una Metodología de Administración de Riesgos en el procedimiento **PGSI-07 Administración del Riesgo**.
- d) Por medio de la Metodología de Administración de Riesgos se tienen identificados los riesgos asociados a los activos de información definidos.
- e) Se analizan y evalúan los riesgos identificados.
- f) Se identifican y evalúan las opciones para el tratamiento de los riesgos identificados.
- g) Se identifican las iniciativas de riesgos a minimizar.
- h) Se determinan los controles adecuados, de acuerdo al objetivo que se pretende lograr con los mismos, justificando su selección en la **Declaración de Aplicabilidad (SoA) FPGSI-07-04**. En caso de ser necesario se seleccionan controles específicos adicionales no incluidos en la Declaración de Aplicabilidad.

- i) La Alta Dirección aprueba los riesgos residuales estimados.
- j) La Alta Dirección autoriza la implementación y operación del SGSI.
- k) La relación de los controles que son aplicables para conseguir el nivel de riesgo residual aprobado por la Alta Dirección se encuentra documentada en la **Declaración de Aplicabilidad (SoA) FPGSI-07-04** (SoA, por sus siglas en inglés, Statement of Applicability)

4.2.2 Implementación y operación del SGSI

Como parte de la implementación y operación del SGSI, la CONSAR realiza las siguientes acciones:


- a) Se formula un plan de tratamiento de riesgos.
- b) Se formulan las iniciativas de riesgos.
- c) Se implementa el plan de tratamiento de riesgos formulado de acuerdo al contenido de este Plan y de las iniciativas de riesgos formuladas.
- d) Se implementan los controles seleccionados.
- e) Se definen indicadores para medir el cumplimiento de los controles seleccionados.
- f) Se concientiza y capacita al personal de la CONSAR incluido en el alcance previamente definido.
- g) Se gestionan los recursos y operaciones del SGSI.
- h) Se implementan procedimientos para responder a incidentes de seguridad.

4.2.3 Monitoreo y revisión del SGSI

Como parte del monitoreo y revisión del SGSI, la CONSAR realiza las siguientes acciones:

- a) Ejecuta el monitoreo y revisión de los procedimientos y controles establecidos en el SGSI.
- b) Realiza revisiones regulares al cumplimiento del SGSI, tomando en cuenta los resultados de las auditorías (interna y externa), resultados del análisis de riesgos, iniciativas derivadas de la revisión anual de la Alta Dirección, incidentes, indicadores, sugerencias y retroalimentación de los involucrados en el SGSI.
- c) Mide el cumplimiento de los controles.
- d) Revisa el análisis de riesgos en intervalos planeados, así como los riesgos residuales.
- e) Conduce revisiones internas al SGSI a intervalos planeados.
- f) Realiza revisiones al SGSI por parte de la Alta Dirección.
- g) Actualiza los planes de seguridad tomando en cuenta los hallazgos encontrados durante las actividades de monitoreo y revisión previamente descritas.
- h) Registra las acciones y eventos que puedan impactar al SGSI.

4.2.4 Mantenimiento y mejora del SGSI

		MANUAL	
		GESTIÓN DE SEGURIDAD DE INFORMACIÓN	
CÓDIGO	FECHA DE REVISIÓN	No. DE REVISIÓN	PÁGINA
MGSI-01	SEPTIEMBRE 2018	14	10 de 37

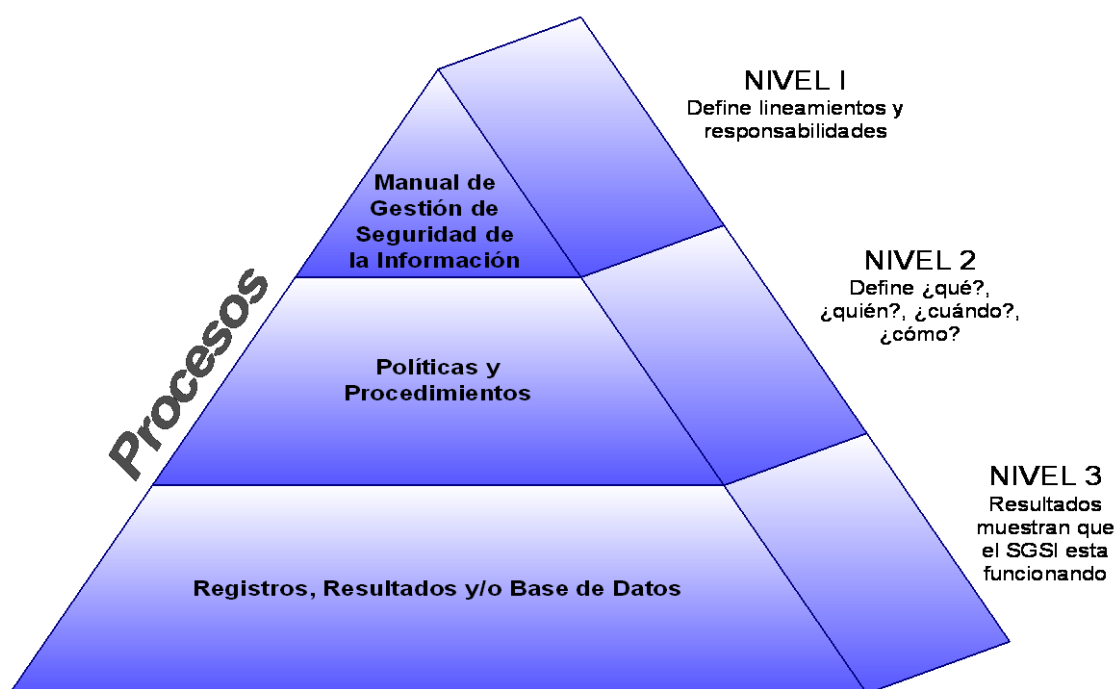
Como parte del mantenimiento y mejora del SGSI, la CONSAR realiza las siguientes acciones:

- Identifica e implementa las mejoras al SGSI.
- Realiza las acciones preventivas y correctivas adecuadas y aplica las lecciones aprendidas de las experiencias de seguridad de información tanto internas como de otras organizaciones.
- Comunica las acciones y mejoras al SGSI a través de los canales definidos para ello.
- Asegura que las mejoras logren los objetivos esperados.

4.3 Requerimientos documentales

4.3.1 General

La **CONSAR** mantiene un Sistema de Gestión de Seguridad de la Información documentado, el cual está estructurado de la siguiente manera:



Documentación Nivel 1:

Manual de Gestión de Seguridad de la Información: Describe el Sistema de Gestión de Seguridad de la Información, la Política, el Alcance y los Objetivos de Seguridad de la Información, las responsabilidades generales para con el sistema y hace referencia a los procedimientos documentados.

Documentación Nivel 2:

Políticas: Establecen las directrices a seguir para cumplir con los objetivos del Sistema de Gestión de Seguridad de la Información. En cada política se definen lineamientos, los cuales describen la mejor forma de implementar y cumplir con las políticas de seguridad de información establecidas. Los lineamientos son una guía de acción.

Procedimientos: Describen las actividades que se realizan para cumplir los requisitos establecidos en la Declaración de Aplicabilidad, definiendo las responsabilidades y las actividades para tal efecto.

Documentación Nivel 3:

Registros: Proporcionan la evidencia objetiva necesaria para demostrar que el Sistema de Gestión de Seguridad de la Información está implantado y opera efectivamente.

Los documentos que integran el Sistema de Gestión de Seguridad de la Información (estructura documental) incluye:

- a. Manual del Sistema de Gestión de Seguridad de la Información.
 - Política de Seguridad de la Información.
 - Alcance del SGSI.
 - Objetivos de Seguridad de la Información.
- b. Procedimientos y registros de seguridad de la información que soporten al SGSI.
- c. Procedimiento de Administración del Riesgos.
- d. Reporte de riesgos identificados.
- e. Plan de tratamiento de riesgos.
- f. Iniciativas de riesgos.
- g. Declaración de Aplicabilidad de Controles.
- h. Procedimientos Operativos y Técnicos.
- i. Registros de los Procesos.
- j. Otros documentos identificados en cada proceso.

4.3.2 Control de documentos

Los documentos del Sistema de Gestión de Seguridad de la Información se controlan mediante el procedimiento **Control de Documentos PGSI-02**, mediante el cual se asegura que los documentos:

- a) Son aprobados previo a su uso.
- b) Son revisados y actualizados conforme sea necesario y nuevamente se vuelven aprobar.
- c) Tienen identificados los cambios y el estatus de la versión actual.
- d) La última versión de los mismos está disponible en los puntos de uso.
- e) Los documentos permanecen legibles y claramente identificables.
- f) Están disponibles para todos aquellos que los necesitan, y son transferidos, almacenados y dispuestos de acuerdo con el procedimiento aplicable a su clasificación.

- g) De origen externo son identificados.
- h) Su distribución está controlada.
- i) Cuando están obsoletos se previene el uso no intencionado de ellos.
- j) Tienen una identificación adecuada si se requiere mantenerlos por cualquier propósito.

4.3.3 Control de registros

El Sistema de Gestión de Seguridad de la Información de la Comisión establece y mantiene el procedimiento **Control de Registros PGSI-03**, el cual define los controles necesarios para la identificación, el almacenamiento, la protección, la recuperación, el tiempo de retención y la disposición de los registros y de esa forma proporcionar evidencia de conformidad con los requisitos de la operación eficaz del Sistema de Gestión de Seguridad de la Información.

Los registros definidos para cada área se encuentran relacionados en la **Lista Maestra de Registros FPGSI-03-01**. Se asegura que los registros permanezcan legibles, fácilmente identificables y recuperables para cualquier uso o consulta.

La Dirección de Informática, tiene definidos mecanismos para el respaldo y protección de la información electrónica de tal forma que se garantice su preservación, consistentes en realizar respaldos y actualizaciones a los servidores.

5 RESPONSABILIDAD DE LA DIRECCIÓN

La Alta Dirección proporciona la evidencia de su participación y compromiso con el desarrollo e implantación del SGSI, así como la mejora continua de su eficacia, a través del seguimiento en las juntas de avance, además de:

- Establecer, comunicar y revisar la Política de Seguridad de Información.
- Garantizar que se establezcan objetivos y planes de Seguridad de Información.
- Proveer recursos suficientes para: constituir, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.
- Aprobar los niveles de riesgos.

Las responsabilidades de la Alta Dirección en cuanto a seguridad de información se refieren y en adición a las actividades que su puesto le confiere son:

- Aprobar los objetivos y planes de seguridad de la información.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a todo el personal de la Comisión involucrado en el alcance del SGSI, la importancia de cumplir con los objetivos de seguridad de la información y la política de seguridad, sus responsabilidades bajo la ley y la necesidad de la mejora continua.
- Garantizar que se conduzcan revisiones internas, coordinando las actividades que se dan entre los integrantes del SGSI y garantizando la participación de los responsables que intervienen en el proceso, mismos que están adscritos a distintas áreas de la Comisión.
- Aprobación de cambios estructurales al SGSI.
- Conducir revisiones de la dirección al SGSI.
- Verificar el cumplimiento de objetivos y planes de seguridad de la información.
- Proveer recursos suficientes para: constituir, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.

5.1 Compromiso de la Dirección

La Alta Dirección se compromete al establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información, el cual es considerado como un mecanismo para proteger la información relacionada con el alcance definido.

5.2 Administración de recursos

5.2.1 Provisión de recursos

La Alta Dirección administra en conjunto con el Coordinador General de Administración y Tecnologías de la Información, que el presupuesto anual asignado incluya los insumos necesarios para:

- a) Establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.
- b) Garantizar que los procedimientos de seguridad de información apoyan los requerimientos de la Comisión.
- c) Identificar y cumplir con los requerimientos legales y regulatorios, así como las obligaciones contractuales de seguridad.
- d) Mantener la seguridad adecuada mediante la correcta aplicación de todos los controles implementados.
- e) Establecer un método para que las políticas y procedimientos se cumplan adecuadamente por el personal de la CONSAR.
- f) Garantizar la renovación tecnológica de hardware y de software para fortalecer la seguridad de la Comisión.
- g) Llevar a cabo revisiones cuando sea necesario, y reaccionar apropiadamente a los resultados de dichas revisiones, y
- h) Cuando se requiera mejorar el cumplimiento del SGSI.

Así mismo, se identifican recursos a través de los resultados de las Revisiones por la Dirección, juntas de trabajo y/o cumplimiento a objetivos de seguridad de la información, resultados del análisis de riesgos y análisis de los indicadores de los controles implementados.

5.2.2 Competencia, toma de conciencia y formación.

La Comisión se asegura de que el personal que tiene asignadas responsabilidades para con el SGSI sea competente para desarrollar las tareas que le fueron requeridas mediante:

- a) Determinar la competencia necesaria para el personal que realiza trabajos que afectan al SGSI, a través de la certificación de capacidades descritas en la descripción, perfil y valuación del puesto.
- b) Proporcionar la capacitación o tomar otras acciones para satisfacer las necesidades identificadas a través de la Detección de Necesidades de Capacitación y de la Evaluación del desempeño.
- c) La Alta Dirección concibe dos tipos de capacitación: La interna que es mediante talleres internos, difusión de trípticos y otros. La externa que es cuando los integrantes del SGSI solicitan cursos de capacitación a impartirse fuera de las instalaciones de la CONSAR por Centros Educativos Especializados, en el cual la logística es coordinada por la Dirección General Adjunta de Recursos Humanos y Presupuesto.
- d) La Dirección General Adjunta de Recursos Humanos y Organización es responsable de mantener los registros que demuestran la capacitación proporcionada, los conocimientos, experiencia, habilidades, educación y los resultados de la certificación de competencias del personal de la Comisión y por consiguiente del personal involucrado en los procesos definidos en el alcance del SGSI.

El personal de la CONSAR que tenga participación en cursos de seguridad deberá estar consciente de la relevancia e importancia de estos y hará uso de lo aprendido para el logro de los Objetivos de Seguridad de la Información.

6 REVISIONES INTERNAS AL SGSI

En el Sistema de Gestión de Seguridad de la Información, cada uno de los procesos y áreas que están dentro de su alcance realizan a intervalos planificados, revisiones internas de seguridad de la información, con el propósito de determinar si el sistema:

- a) Es conforme con los requisitos establecidos en la normatividad aplicable.
- b) Es conforme con los requisitos de seguridad de información identificados y establecidos por la CONSAR.
- c) Se ha implementado, se mantiene y se ejecuta de forma efectiva.
- d) Se desarrolla conforme se esperaba.

Para realizar dichas revisiones, se cuenta con el procedimiento de **Revisiones Internas PGSI-04**, en donde se definen las actividades para la planeación y programación de las revisiones, tomando en consideración el estado e importancia de los procesos y las áreas a revisar, así como los resultados de revisiones previas, define también los criterios de revisión, alcance y metodología.

Están definidos de igual forma las responsabilidades y requisitos para la planificación y realización de revisiones, y se muestra el método para comunicar los resultados obtenidos para la toma de acciones oportunas, y los registros que deben resultar de la revisión.

Una vez que se informan los resultados de la revisión a la Alta Dirección y a los Responsables de Proceso, se ejecutan las acciones comprometidas, para eliminar las deficiencias detectadas y sus causas; tomando como referencia el procedimiento de **Acciones Correctivas, Preventivas o de Mejora PGSI-05**, donde las actividades de seguimiento incluyen la verificación de las acciones tomadas y el informe de los resultados de la verificación.

7 REVISIÓN GERENCIAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

7.1 Generalidades

En cuanto al SGSI, la Alta Dirección realiza una revisión del sistema una vez al año a fin de asegurar su conveniencia, adecuación y eficacia. En la revisión se evalúan las oportunidades de mejora y la necesidad de cambios, incluyendo las políticas de seguridad de información y los objetivos de seguridad de información.

7.2 Entradas a la revisión

La información que se utiliza como elementos de entrada en la Revisión por la Alta Dirección se notifica a través de una agenda, considerando lo siguiente:

- a) Resultados de revisiones al SGSI.
- b) Resultados del análisis de riesgos.
- c) Retroalimentación de las partes interesadas (propuestas y sugerencias recibidas o implementadas para mejora en conceptos de seguridad de la información por parte del personal involucrado en el alcance del SGSI).
- d) Técnicas, productos o procedimientos que puedan ser utilizados para mejorar el desempeño, el cumplimiento del Sistema de Gestión de Seguridad de la Información.
- e) Estatus de las acciones preventivas y correctivas.
- f) Vulnerabilidades o amenazas detectadas en la revisión, operación u otro medio que no hayan sido plenamente mitigadas en el análisis de riesgos anterior.
- g) Resultados de la medición del cumplimiento de los controles implementados.
- h) Acciones de seguimientos derivadas de revisiones previas.
- i) Cambios que pudieran afectar al Sistema de Gestión de Seguridad de la Información.
- j) Recomendaciones de mejora recibidas por parte del personal involucrado en el alcance del SGSI u otros.

Los resultados derivados de la revisión por la Alta Dirección son registrados en la **Minuta de la Junta de la Revisión por la Dirección FMGSI-01-01** donde se establecen los acuerdos tomados, los responsables para cada acuerdo y los plazos de cumplimiento a los compromisos generados.

7.3 Resultados de la revisión

Los resultados de la Revisión por la Alta Dirección, incluyen cualquier decisión y acciones relacionadas con lo siguiente:

- a) Mejoras al cumplimiento del SGSI
- b) Actualización del análisis de riesgos y del plan de tratamiento de riesgos.

- c) Modificación a los procedimientos y controles que afectan a la seguridad de la información, conforme sea necesario, para responder a los eventos internos o externos que puedan impactar al SGSI, incluyendo cambios en:
- 1) Requerimientos de la CONSAR.
 - 2) Requerimientos de seguridad.
 - 3) Procesos de la CONSAR que afecten los requerimientos existentes.
 - 4) Requerimientos legales y/o regulatorios.
 - 5) Obligaciones contractuales.
 - 6) Niveles de riesgos y/o criterios para aceptar los riesgos.
- d) Recursos necesarios
- e) Mejora sobre cómo se mide el cumplimiento de los controles.

Dependiendo de la complejidad de la acción a tomar se puede decidir documentarla en función de lo que establece el procedimiento de **Acciones Correctivas, Preventivas o de Mejora PGSI-05**.

El Responsable del SGSI da seguimiento al cumplimiento e implantación de los acuerdos, decisiones y acciones, anexando las evidencias correspondientes y notificando de los avances a la Alta Dirección.

7.4 Proceso de Seguimiento a Revisión de la Alta Dirección

Todos los registros definidos en la Minuta de la Junta de la Revisión por la Dirección FMGSI-01-01 deberán ser incluidos en el Reporte de Seguimiento a la Revisión de la Alta Dirección FMGSI-01-02.

Se determinan las fechas probables de Inicio y Término en que se planea dar solución a cada iniciativa propuesta.

Se programan las fechas en las que se revisará el programa de Seguimiento a la Revisión de la Alta Dirección FMGSI-01-02.

8 MEJORA DEL SGSI

8.1 Mejora continua

La Alta Dirección mejora continuamente el Sistema de Gestión de Seguridad de la Información emprendiendo acciones para eliminar los hallazgos de las revisiones e implementa la mejora continua del SGSI mediante:

- a) El uso de la política de seguridad de la información.
- b) Los objetivos de la seguridad de la información.
- c) Los indicadores de cumplimiento de los procesos que intervienen en el SGSI.
- d) Los resultados de las revisiones de seguridad internas.
- e) Los resultados del análisis de riesgos.
- f) Las acciones correctivas y preventivas.
- g) La revisión por la Dirección.

8.2 Acción correctiva

Dentro del Sistema de Gestión de Seguridad de la Información se aplican las acciones correctivas de acuerdo al procedimiento de **Acciones Correctivas, Preventivas o de Mejora PGSI-05**, necesarias para eliminar las causas de las deficiencias en la implementación, operación y uso del SGSI con el objetivo de prevenir su recurrencia.

En el procedimiento de **Acciones Correctivas, Preventivas o de Mejora PGSI-05** se definen los requerimientos para:

- a) Identificar deficiencias y deficiencias potenciales y sus causas.
- b) Determinar la causa de las deficiencias.
- c) Evaluar la necesidad de tomar acciones para evitar que las deficiencias se vuelvan recurrentes.
- d) Evaluar la necesidad de tomar acciones preventivas para evitar la ocurrencia de deficiencias.
- e) Determinar e implementar las acciones correctivas y/o preventivas necesarias.
- f) Registrar los resultados de las acciones tomadas.
- g) Revisar las acciones correctivas y/o preventivas tomadas.

8.3 Acción preventiva

El procedimiento de **Acciones Correctivas, Preventivas o de Mejora PGSI-05**, además de aplicarse a acciones correctivas se utiliza también para acciones de mejora y preventivas. Sirve para establecer el método que determina las acciones para la mejora o prevención que ayudan a mejorar el sistema y para prevenir que se presente en el futuro alguna deficiencia.

Para el caso de que el procedimiento de **Acciones Correctivas, Preventivas o de Mejora PGSI-05** sea utilizado como mejora o prevención dentro del SGSI, se deben definir los requerimientos para:

- a) Identificar las áreas de mejora o de prevención.
- b) Determinar e implementar las acciones preventivas necesarias
- c) Registrar los resultados de las acciones tomadas
- d) Revisar las acciones preventivas tomadas

9. REFERENCIAS:

9.1 Marco Normativo:

Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y en la de Seguridad de la Información (MAAGTICSI)

9.2 Documentos:

Código	Documento
PGSI-02	Control de Documentos
PGSI-03	Control de Registros
PGSI-04	Revisiones Internas
PGSI-05	Acciones correctivas, preventivas o de mejora
PGSI-07	Administración de Riesgos

9.3 Formatos:

Código	Documento
FMGSI-01-01	Minuta de la Junta de la Revisión por la Dirección
FMGSI-01-02	Reporte de Seguimiento a la Revisión de la Alta Dirección
FPGSI-02-01	Lista Maestra de Documentos Controlados
FPGSI-03-01	Lista Maestra de Registros
FPGSI-07-04	Declaración de Aplicabilidad (SoA)

10. GLOSARIO DE TÉRMINOS Y DEFINICIONES

AAR: Conjunto Activo-Amenaza-Riesgo.

Acción Correctiva: Acción tomada para eliminar las causas de una deficiencia detectada u otra situación indeseable.

Acción Preventiva: Acción tomada para eliminar las causas de una deficiencia u otra situación potencialmente indeseable.

Aceptación del riesgo: Es la decisión de aceptar un nivel de riesgo de tal forma que la Comisión opere conviviendo con éste.

Activo: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Administración del riesgo: Conjunto de actividades coordinadas para dirigir y controlar una organización en referencia al riesgo.

Alta Dirección: Es la máxima autoridad del Sistema de Gestión y tiene como su responsabilidad que los conceptos de Seguridad se apliquen correctamente en la CONSAR.

Amenaza: Causa potencial de un incidente no planeado, el cual puede resultar en daño a un sistema u organización.

Análisis de riesgo: Proceso que permite la identificación de las amenazas que acechan a los activos, para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.


Anexo: Documento que describe con más detalle el desarrollo de algún proceso o actividad, que contiene toda la información de referencia de concepto o que proporciona información relacionada al contexto que se está describiendo en el documento original.

Auditor: Persona con la competencia para llevar a cabo una Auditoría.

Revisor: Empleado de la propia institución con los conocimientos de los procesos, procedimientos y en general con la competencia para llevar a cabo una Revisión.

CID: Confidencialidad, Integridad, Disponibilidad

Cinco pasos para la solución de problemas: Proceso disciplinado para el análisis de situaciones para determinar y eliminar las causas de no conformidades reales y potenciales.

		MANUAL	
		GESTIÓN DE SEGURIDAD DE INFORMACIÓN	
CÓDIGO	FECHA DE REVISIÓN	No. DE REVISIÓN	PÁGINA
MGSI-01	SEPTIEMBRE 2018	14	21 de 37

CISO: Oficial de Seguridad de la Información (Chief Information Security Officer).

Confidencialidad: Aseguramiento de que la información es accesible solo por aquellos autorizados a tener acceso.

Comisión: Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR).

Control: Práctica, procedimiento o mecanismo que reduce el nivel de riesgo.

Criterios para la revisión: Conjunto de políticas, procedimientos o requisitos utilizados como referencia.

Cumplimiento: Actuación que se lleva a cabo como consecuencia de una obligación, una promesa o una orden.

Debilidad o Deficiencia: Para efectos del Sistema de Gestión de Seguridad de la Información, una debilidad es cuando se detecta algún elemento que ponga en riesgo el ciclo de vida del SGSI, que bien puede ser un procedimiento mal definido que no lleve el SGSI a nada concreto o falta de evidencias o falta de herramientas para el soporte del SGSI. Por ejemplo una debilidad se aprecia cuando sucede cualquiera de los siguientes puntos: Falta de capacitación en los usuarios, utilización de contraseñas débiles, uso de tecnología no probada, falta de un control de cambios integral para toda la infraestructura tecnológica

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Documento Controlado: Cualquier documento que por su relevancia puede, en cualquier momento dado, afectar la seguridad o poner en riesgo la seguridad y el cumplimiento de los requisitos especificados; por lo tanto, debe ejercerse sobre él un control estricto de las versiones y copias que se emitan.


Documento No Controlado: Es aquel que no necesita un control estricto de las versiones y copias que se emiten, pero que deben identificarse.

Documento Obsoleto: Es aquel que derivado de un cambio o emisión pierde su vigencia.

Efectividad: Es la capacidad de lograr el efecto que se desea o se espera con el mínimo de recursos posibles.

Esfuerzo Notable: Presencia de evidencias que manifiestan un trabajo sobresaliente, especialmente atendido y/o cuidadosamente tratado, que resultó en un amplio resultado para preservar la confidencialidad, integridad o disponibilidad de cierta información sensible.

Evidencia Objetiva: Datos que respaldan la existencia o veracidad de algo.

		MANUAL	
		GESTIÓN DE SEGURIDAD DE INFORMACIÓN	
CÓDIGO	FECHA DE REVISIÓN	No. DE REVISIÓN	PÁGINA
MGSI-01	SEPTIEMBRE 2018	14	22 de 37

Formato: Diseño o estructura predeterminada en la que se incorpora la descripción de datos de evidencia de un proceso u operación, que puede estar diseñado en una hoja de papel o en un medio electrónico.

Gestión del riesgo: Proceso basado en los resultados obtenidos en el análisis de riesgo, que permite seleccionar e implantar las medidas o controles de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados reduciendo de esta manera al mínimo su potencialidad o posibles perjuicios.

Guía: Documento de referencia con un objetivo específico para el desarrollo de una actividad, proporcionando una explicación a detalle de cada concepto tratado.

Hallazgos: Resultados de la evaluación de la evidencia de la revisión recopilada frente a los criterios utilizados.

Incidente: Un incidente es un suceso que afecta directamente los activos informáticos y que pone en riesgo la seguridad de la información, como puede ser que una computadora contenga un virus, un spyware, un exploit, etc.

Integridad: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

ISO: Oficial de Seguridad de Información que ejecuta tareas técnicas y operativas (Information Security Officer)


Legible: Que se permita su clara lectura.

Manual de Gestión de Seguridad de la Información: Es el documento que establece la Política de Seguridad de la Información y describe el Sistema de Gestión de Seguridad de la Información de una Organización.

Deficiencia: Es el incumplimiento de un requisito especificado en el Sistema de Gestión de Seguridad de la Información.

Deficiencia Mayor: Ausencia o fallo de uno o varios requerimientos que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

Deficiencia Menor: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

		MANUAL	
		GESTIÓN DE SEGURIDAD DE INFORMACIÓN	
CÓDIGO	FECHA DE REVISIÓN	No. DE REVISIÓN	PÁGINA
MGSI-01	SEPTIEMBRE 2018	14	23 de 37

Observación: Situación aislada que, basada en evidencias objetivas, demuestra una pequeña desviación de algún aspecto de un requerimiento de control, el cual podrá ser adecuado o completado para preservar la confidencialidad, integridad o disponibilidad de la información.

Oportunidad de Mejora: Situación que cumple adecuadamente con el requerimiento de control, sin embargo, es susceptible de mejora para ser más eficiente en el proceso identificado, sin descuidar el objetivo que lo origina.

Procedimiento: Forma específica de desarrollar una actividad. Los procedimientos están documentados y representan el segundo nivel de la documentación del Sistema de Gestión de Seguridad de la Información.

Proceso: Es un conjunto de actividades que suceden de forma ordenada a partir de la combinación de materiales, equipo, gente, métodos y medio ambiente, para convertir insumos en productos o servicios con valor agregado.

Registro: Información documentada que provee evidencia objetiva de las actividades ejecutadas o resultados obtenidos.

Requerimiento de Seguridad: Necesidad de establecer un control a algún activo para disminuir el riesgo identificado.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia.

Riesgo Residual: Es el riesgo que permanece después de que la Comisión realiza el tratamiento de los riesgos identificados como parte del proceso de Administración del Riesgo, es decir, es el riesgo que permanece después de implementar los controles seleccionados.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información

Sistema: Es un conjunto de elementos que permanecen unidos porque continuamente se afectan unos a otros en el transcurso del tiempo y funcionan para obtener un propósito común.

Sistema de Gestión de Seguridad de la Información: Es un sistema de gestión que comprende la política, la estructura organizacional, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información. Este sistema es la herramienta de que dispone la Dirección General para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.)

SoA: Declaración de Aplicabilidad (Statement of Applicability, SoA por sus siglas en inglés).

Tratamiento del Riesgo: Proceso de selección e implementación de controles para modificar el riesgo.

Valor de los Activos: Se establece como el valor asignado a los activos tangibles e intangibles, en base a la importancia que tienen para la empresa con el propósito de lograr sus objetivos generales. El valor puede estar basado en un cálculo de lo que podría ser el valor comercial del activo en términos de productividad y beneficio.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

ANEXO I

Un **Indicador** es una magnitud asociada a una característica (del resultado, del proceso, de las actividades, de la estructura, etc.) que permite a través de su medición en periodos sucesivos y por comparación con el estándar establecido, evaluar periódicamente dicha característica y verificar el cumplimiento de los objetivos (estándares) establecidos. Algunos indicadores sólo reflejan el resultado de la ejecución de una acción.

Para el SGSI de la CONSAR se establecen 3 tipos de indicadores: Estructura, Cumplimiento y Efectividad.

Indicadores de Estructura: Registran el resultado de la ejecución de una tarea o acción, no están basados en ningún estándar o valor preestablecido al cual se pretenda llegar. Su objetivo es llevar un control de tareas, que aunque sean cuantificables, no son representativos para el desarrollo y madurez del SGSI, pero permiten llevar un control y tener un orden. Dependiendo de la información que reflejen, la cual pueda ser enriquecida con otros datos y/o valores, pueden evolucionar a un indicador de cumplimiento.

Indicadores de Cumplimiento: Registran el cumplimiento de una acción o actividad encomendada o planeada. Persiguen el cumplimiento de un valor preestablecido al que se pretenda alcanzar, el cual puede aumentar o disminuir según su complejidad o madurez en el sistema. De manera mínima o prácticamente nula considera aspectos de calidad, beneficios, resultados o consecuencias. Dependiendo de la información que reflejen, la cual puede ser enriquecida con otros datos y/o valores y pueden evolucionar a un indicador de efectividad.

Indicadores de Efectividad: Son indicadores de cumplimiento mejorados, incluso en la mayor parte de los casos derivan de dichos indicadores. Más allá de solo registrar y reflejar si se cumple o no la tarea o acción, hacen un análisis de los valores que contiene el indicador, de tal manera que cubre en mayor grado aspectos de calidad, beneficios, resultados o consecuencias. Son una fuente confiable para toma de decisiones del proceso que se esté midiendo, ya que permiten analizar, entre otros temas, el comportamiento de un proceso en el tiempo o hacer una revisión más exhaustiva de un proceso que pueda ser afectado por muchas variables.

MEDICIÓN DE LOS INDICADORES DEL SGSI

Núm	Tipo de Indicador	Nombre del Indicador	Documento Mandatorio	Periodicidad
1	Estructura	Control de Altas y Bajas de Usuarios en Active-Directory	PDGI-09	Mensual
2	Estructura	Control de Altas y Bajas de Usuarios en BD	PDGI-09	Mensual
3	Estructura	Registro de Fallos del Sistema OSIRIS ¹	PDGI-46	Mensual
4	Estructura	Integración de la BD del Sistema OSIRIS ¹	PDGI-46	Mensual
5	Estructura	Archivos procesados en el sistema ISIS	PDGI-47	Mensual
6	Estructura	Control de modificación de documentos del SGSI ¹	PGSI-02	Trimestral
7	Estructura	Control de Solicitudes de Acciones ¹	PGSI-05	Trimestral
8	Cumplimiento	Reuniones del personal designado como ISO del SGSI ¹	MSGSI Punto 7	Cuatrimestral
9	Cumplimiento	Revisiones Internas ¹	PGSI-04	Anual
10	Cumplimiento	Capacitación en Seguridad de Información	PDGI-04	Semestral
11	Cumplimiento	Pruebas de Vulnerabilidades ¹	PDGI-24	Cuatrimestral
12	Cumplimiento	Incidentes de Seguridad de Información ¹	PDGI-43	Mensual
13	Cumplimiento	Mantenimiento Preventivo ¹	PDGI-25, PDGI-27, PDGI-29, PDGI-31, PDGI-33, PDGI-35	Mensual
14	Cumplimiento	Pruebas del DRP ¹	PDGI-48	Anual
15	Cumplimiento	Envío de medios a Bóveda de Seguridad	PDGI-20	Mensual
16	Efectividad	Respaldos de Información ¹	PDGI-18	Mensual
17	Efectividad	Actualización de Antivirus ¹	PDGI-06	Mensual
18	Efectividad	Actualizaciones de Seguridad Windows a Equipos de Usuarios ¹	PTDGI-01	Mensual

Núm	Tipo de Indicador	Nombre del Indicador	Documento Mandatorio	Periodicidad
19	Efectividad	Actualizaciones de Seguridad Windows a Servidores ¹	PTDGI-01	Mensual
20	Efectividad	Solución a Fallos del Sistema OSIRIS ¹	PDGI-46	Mensual

Nota: Todos los indicadores tienen una Gráfica de cumplimiento como Registro de Evidencia.

¹ Estos indicadores tienen otros documentos como evidencias (reportes, minutas, bitácoras, etc.)

Los **Indicadores** se deben generar con la periodicidad establecida para cada uno de ellos y deberán cumplir su meta de cumplimiento establecida. El responsable del proceso del cual emanan los datos para la creación del indicador, también será el responsable del cumplimiento de esta medición hasta la validación de su difusión en el SGSI.

Con el objetivo de mantener control sobre la generación de los indicadores de acuerdo a su periodicidad o bien que las métricas definidas para cada uno de ellos se cumplan, se elaborará una Solicitud de Acción bajo las siguientes condiciones:

Si un indicador tiene periodicidad:

- Mensual y acumula 3 periodos sin elaborarse o 3 periodos sin que se alcance la métrica establecida.
- Trimestral o Cuatrimestral y acumula 2 periodos sin elaborarse o 2 periodos sin que se alcance la métrica establecida.
- Semestral o Anual y no se elabora máximo 30 días después de la fecha en que debió elaborarse o no cumple con la métrica establecida.

La Solicitud de Acción buscará documentar el retraso para que sea corregido a la brevedad y en el caso de incumplimiento de métricas se debe determinar si es posible volver al cumplimiento de la meta establecida o se deberá redefinir la métrica.

La Solicitud de Acción deberá firmarse por el responsable del proceso, el jefe inmediato superior de éste último y el responsable del SGSI. Se dará seguimiento a la Solicitud de Acción hasta el cierre de la misma que será cuando se regularice la situación de faltantes y/o que el indicador regrese a sus niveles de cumplimiento mínimos.

DESCRIPCIÓN DE LOS INDICADORES DEL SGSI

Núm	Indicador	Objetivo	Medición	Unidad de Medida	Período	Meta	Responsable de Medirlo	Objetivos Soportado	Observaciones
1	Control de Altas y Bajas de Usuarios en Active – Directory	Garantizar que los movimientos de Altas y Bajas de usuarios en Active – Directory se realizan correctamente en tiempos adecuados.	Registro de Altas y Bajas de Usuarios de Active-Directory	#	Mensual	N/A	Subdirector de Infraestructura	4, 5	El control oportuno del registro de los movimientos de Altas y Bajas de Usuarios en Active – Directory para asegurar el acceso a los procesos solo a personal activo de la CONSAR.
2	Control de Altas y Bajas de Usuarios en BD	Garantizar que los movimientos de Altas y Bajas de usuarios en BD se realizan correctamente en tiempos adecuados.	Registro de Altas y Bajas de Usuarios en BD	#	Mensual	N/A	Subdirector de Infraestructura	4, 5	El control oportuno del registro de los movimientos de Altas y Bajas de Usuarios en BD para asegurar el acceso a los procesos solo a personal activo de la CONSAR.
3	Registro de Fallos del Sistema OSIRIS	Identificar el tipo y la frecuencia de fallos al proceso de Recepción y su oportuna corrección.	Registro de Fallos del Sistema OSIRIS	#	Mensual	N/A	Administrador del Sistema OSIRIS	2, 4, 5	La oportuna atención de cualquier fallo en el proceso de recepción garantiza la disponibilidad e integridad de la información.
4	Integración de la BD del Sistema OSIRIS	Monitoreo de los archivos que se deben de recibir a manera de llevar un registro para identificar el volumen de información recibida.	Registro de Número de Archivos Integrados a la BD del Sistema OSIRIS	#	Mensual	N/A	Administrador del Sistema OSIRIS	4, 5	El registro de los archivos recibidos así como espacio de almacenamiento, para prever el crecimiento y supervisión de estos.

Núm	Indicador	Objetivo	Medición	Unidad de Medida	Período	Meta	Responsable de Medirlo	Objetivos Soportado	Observaciones
5	Archivos procesados en el sistema ISIS	Identificar la cantidad de archivos recibidos mediante el proceso con Información a Detalle	Registro de número de archivos procesados en el mes	#	Mensual	N/A	Líder de Proyecto	1, 2	Sustentar e identificar áreas de mejora al sistema de procesamiento de archivos.
6	Control de modificación de documentos del SGSI	Asegurar que los documentos del SGSI se mantienen actualizados y son vigentes	Registro de número de modificaciones a documentos solicitadas y concluidos en el periodo	#	Trimestral	N/A	Responsable del SGSI	2, 5	Una documentación siempre actualizada y bien hecha permite a los involucrados contar con herramientas de trabajo para la recepción de información, lo que garantiza la continuidad operativa y minimiza el impacto de incidentes.
7	Control de Solicitudes de Acciones	Mejorar el desempeño del SGSI a través de acciones correctivas, preventivas y de mejora	Registro de número de Solicitudes de acción generadas y cerradas en el periodo	#	Trimestral	N/A	Revisor	2, 5	Las solicitudes de acción pueden ser de corrección o mejora al SGSI. Son controles o documentos que permiten mejorar el proceso para garantizar la continuidad operativa y minimizar el impacto de incidentes, ya que un proceso de mejora continua implementa mejores controles.

Núm	Indicador	Objetivo	Medición	Unidad de Medida	Período	Meta	Responsable de Medirlo	Objetivos Soportado	Observaciones
8	Reuniones del personal designado como ISO del SGSI	Garantizar que las actividades de seguridad de información están siendo coordinadas por representantes de las diferentes áreas de la Comisión que tienen un rol relevante para el alcance del SGSI	(Reuniones celebradas del personal designado como ISO / Reuniones programadas del personal designado como ISO) * 100	%	Cuatrimstral	75%	Director de Informática	1, 3, 5	El Comité de seguridad de información hace notar a los miembros e invitados el valor de la información y resalta la importancia que implica para el desarrollo de las funciones de todas las áreas. Promueve una cultura de seguridad por medio de los documentos generados y nuevos proyectos a implementar. Produce la reducción de los incidentes de seguridad de la información.
9	Revisiones Internas	Determinar si el SGSI cumple con los requisitos establecidos, se mejora continuamente y se mantiene de manera eficaz	(Revisiones realizadas / Revisiones programadas) * 100	%	Anual	85%	Revisor	2	Las revisiones permiten promover que los controles y documentación relacionada se lleve a cabo, garantizando la continuidad del proceso.

Núm	Indicador	Objetivo	Medición	Unidad de Medida	Período	Meta	Responsable de Medirlo	Objetivos Soportado	Observaciones
10	Capacitación en Seguridad de Información	Contar con personal competente en el puesto indicado, así como garantizar que el personal está consciente y capacitado en las políticas y procedimientos de seguridad de la información	(Número de actividades de capacitación ejecutadas / Número de actividades de capacitación programadas) * 100	%	Semestral	90%	Jefe de Departamento de Innovación, Estructuras y Capacitación	2, 3, 4	La capacitación permite promover una cultura de seguridad y protección. Crea conciencia respecto a la seguridad de los activos y conoce más su proceso y sus controles, por lo que sus trabajos van orientados a garantizar la continuidad y a mantener el CID de la información. Se promueve a través de cursos, difusión en Intranet, papel tapiz de la computadora, protector de pantalla de la computadora y trípticos.
11	Pruebas de Vulnerabilidades	Asegurar el cumplimiento de los sistemas y aplicaciones con las políticas y procedimientos de seguridad de información establecidos	(Pruebas de vulnerabilidades ejecutados / Pruebas de vulnerabilidades programados) * 100	%	Cuatrimstral	85%	Subdirector de Infraestructura	4, 5	Las pruebas de penetración y de identificación de vulnerabilidades, ayudan a corregir huecos de seguridad que pudieran afectar el proceso de recepción de información. La práctica continua de estas pruebas mantiene el CID de la información y minimizan los incidentes de seguridad.

Núm	Indicador	Objetivo	Medición	Unidad de Medida	Período	Meta	Responsable de Medirlo	Objetivos Soportado	Observaciones
12	Incidentes de Seguridad de Información	Garantizar que los incidentes de seguridad de información son reportados en tiempo y forma, permitiendo tomar las acciones correctivas pertinentes	(Incidentes de seguridad de información resueltos / Incidentes de seguridad de información reportados) * 100	%	Mensual	90%	Subdirector de Infraestructura	5	La continua comunicación sobre los incidentes de seguridad detectados permite a la CONSAR actuar de manera oportuna y poder tomar decisiones proactivas a futuro, lo que ayuda a la minimización de incidentes.
13	Mantenimiento Preventivo	Prevenir pérdida o daño a los equipos informáticos e interrupción de los procesos de la Comisión, garantizando su continua disponibilidad e integridad	(Mantenimientos preventivos ejecutados / Mantenimientos preventivos programados) * 100	%	Mensual	85%	Subdirector de Infraestructura	2, 4, 5	El plan de mantenimientos preventivos y correctivos a los activos de hardware permite garantizar la continuidad del proceso, minimizar incidentes y sobre todo mantener la disponibilidad e integridad de dichos activos.
14	Pruebas del DRP	Asegurar que el Plan de Recuperación de Desastres (DRP) esté vigente y que el personal esté preparado conociendo su rol y los sistemas e información estén recuperables y actualizados en un sitio alternativo	(Pruebas del DRP realizadas / Pruebas del DRP programadas) * 100	%	Anual	60%	Director de Informática	2, 4	El DRP por sus características de ser un sitio alternativo con comunicación de una red privada, garantiza la confidencialidad y disponibilidad de la información y la continuidad de la operación del proceso de recepción de información.

Núm	Indicador	Objetivo	Medición	Unidad de Medida	Período	Meta	Responsable de Medirlo	Objetivos Soportado	Observaciones
15	Envío de medios a Bóveda de Seguridad	Asegurar que existe un respaldo externo para prevenir la falta de información.	(Envíos a Bóveda ejecutados / Envíos a Bóveda programados) *100	%	Mensual	75%	Subdirector de Infraestructura	2, 4, 5	Los respaldos enviados a Bóveda de Seguridad garantizan la continuidad del proceso de recepción de información en caso de existir algún evento de contingencia.
16	Respaldos de Información	Prevenir la pérdida y falta de disponibilidad de la información	Automática : ((Respaldos programados - con falla) / Respaldos programados) * 100 Total : ((Respaldos programados - con falla + relanzados) / Respaldos programados) * 100	%	Mensual	Automática : 90% Total : 95%	Administrador de Base de Datos	2, 4	Los respaldos permiten garantizar la continuidad operativa ante un evento de falla, siendo posible la recuperación la información con que se trabaja, por lo que el CID de información se mantiene soportado.

Núm	Indicador	Objetivo	Medición	Unidad de Medida	Período	Meta	Responsable de Medirlo	Objetivos Soportado	Observaciones
17	Actualización de Antivirus	Proteger la integridad de los equipos, servidores y su información contenida, mediante la detección y prevención de virus.	(Total de equipos actualizados con EPO / (Total de equipos - Equipos no contemplados)) * 100	%	Mensual	92%	Líder de Proyecto	1, 2, 4, 5	El antivirus institucional se maneja a nivel de cliente PC, a nivel de servidores Windows y a nivel de correo corporativo, por lo que la protección contra virus es bastante robusta y permite que haya operación, que el CID de la información no se vea afectado y que se minimicen los incidentes de seguridad.
18	Actualizaciones de Seguridad Windows a Equipos de Usuarios	Proteger la integridad de los equipos y su información contenida, mediante la prevención de posibles ataques a nuevas vulnerabilidades de los Sistemas Operativos Windows.	(Total de equipos actualizados con WSUS / (Total de Equipos - Equipos no contemplados)) *100	%	Mensual	92%	Líder de Proyecto	1, 2, 4, 5	La instalación de actualizaciones de seguridad se hace de forma remota y centralizada para los equipos de los usuarios, proporcionando una protección más robusta y controlada.
19	Actualizaciones de Seguridad Windows a Servidores	Proteger la integridad de los equipos y su información contenida, mediante la prevención de posibles ataques a nuevas vulnerabilidades de los Sistemas Operativos Windows.	Total de servidores actualizados con WSUS / (Total de servidores - Servidores no contemplados)) *100	%	Mensual	92%	Líder de Proyecto	1, 2, 4, 5	La instalación de actualizaciones de seguridad se hace de forma remota y centralizada para los equipos servidores, proporcionando una protección más robusta y controlada.

Núm	Indicador	Objetivo	Medición	Unidad de Medida	Período	Meta	Responsable de Medirlo	Objetivos Soportado	Observaciones
20	Solución a Fallos del Sistema OSIRIS	Registrar los tiempos de respuesta a problemas suscitados a manera de no rebasar los límites establecidos para su solución y así garantizar la disponibilidad e integridad de la información.	Prom Σ ((Hora Detección + Tiempo de Solución) * Valoración de Servicio)	#	Mensual	8.0	Administrador del Sistema OSIRIS	4, 5	Indicador que sirve para verificar el tiempo efectivo que tardo el ingeniero en solucionar el problema detectado.

CONTROL DE CAMBIOS

No. DE REVISIÓN	FECHA	MOTIVO
14	Septiembre 2018	Se agrega reseña histórica de la evolución del SGSI. Se suprimen las referencias al ISO 27001 excepto en la sección de la reseña histórica del SGSI.
13	Enero 2013	Se agrega situaciones de incumplimiento en la elaboración de los indicadores. Se modifican algunos parámetros en la tabla de indicadores para lograr su cumplimiento. Los indicadores de "Control de modificación de documentos del SGSI" y "Control de Solicitudes de Acciones" se cambian a tipo Estructura.
12	Mayo 2011	Se agrega el punto "7.4 Proceso de Seguimiento a Revisión de la Alta Dirección" en el que se hace referencia al "FMGSI-01-02 Reporte de Seguimiento a la Revisión de la Alta Dirección"
11	Enero 2011	Se agrega el indicador "Archivos procesados en el sistema ISIS" de tipo Estructura con periodicidad Mensual en el Anexo I.
10	Agosto 2010	En el Anexo I: Se modifica el indicador "Actualización de Antivirus" a Efectividad. Se agregan los indicadores "Actualizaciones de Seguridad Windows a Equipos de Usuarios" y "Actualizaciones de Seguridad Windows a Servidores". Se ajusta la información definida en los indicadores de tipo Estructura. Se ordena la lista de indicadores agrupándolos por tipo de indicador.
09	Junio 2010	Se modifica el indicador "Respallos de Información" para convertirlo a Efectividad Se corrige la periodicidad con la que se elabora el indicador "Reuniones del personal designado como ISO del SGSI" en el Anexo I.
08	Mayo 2010	Se modifica la fórmula de medición del indicador "Registro de Fallos del Sistema OSIRIS" Se agregan los indicadores "Solución a Fallos del Sistema OSIRIS" e "Integración de la BD del Sistema OSIRIS". Se agrega una descripción de los indicadores en el Anexo I

MANUAL

GESTIÓN DE SEGURIDAD DE INFORMACIÓN

CÓDIGO
FECHA DE REVISIÓN
No. DE REVISIÓN
PÁGINA
MGSI-01
SEPTIEMBRE 2018
14
37 de 37

No. DE REVISIÓN	FECHA	MOTIVO
07	Noviembre 2009	Se cambia la periodicidad de elaboración del indicador "Cumplimiento de Actualización de Antivirus" de Cuatrimestral a Bimestral. Se agrega el nuevo indicador de "Cumplimiento del Control de Altas y Bajas de Usuarios en BD" Se ajustan diversos párrafos para definir los conceptos de forma más específica.
06	Agosto 2009	Se elimina la sección Términos y Definiciones y se crea la nueva sección de Glosario en la que se agrupan todos los términos utilizados en este documento y en los Procedimientos de Gestión. Se cambia el término Efectividad por Cumplimiento en todo el documento. Se modifica Anexo I : Medición del Cumplimiento en los Controles, para agregar 3 nuevos controles.
05	Noviembre 2008	Se modifica Anexo I : Medición en la Efectividad en los Controles, para ajustar las Metas de Cumplimiento de todos los indicadores a valores más reales de cumplir. Se modifica la fórmula de evaluación del indicador de Reuniones del Comité.
04	Mayo 2008	Se modifica el punto "7.2 Entradas a la revisión", para ser más específico respecto a quien realiza la retroalimentación del SGSI.
03	Noviembre 2007	Se modifica el punto 5, de Responsabilidades de la Dirección, que señala al Director de Operación de Sistemas como Alta Dirección, se ajusta el texto para futuros cambios de personal y puestos para que siempre se refiera a la Alta Dirección como tal.
02	Mayo 2007	Cambio del Anexo I : Medición en la Efectividad en los Controles. Se reordenaron en base a la estructura documental del SGSI, se ajustaron las descripciones de los indicadores, se mejoraron las descripciones de sus objetivos y observaciones y se modificaron en algunos, sus fórmulas de medición y su periodicidad de medición.
01	Diciembre 2006	Numeración de los objetivos de seguridad de la información y asociación de los mismos con la medición de la efectividad de los controles seleccionados.
00	Junio 2006	Creación del Manual del Sistema de Gestión de Seguridad de la Información