MANUAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

TIPO DE DOCUMENTO: Manual

CÓDIGO: MAN GSI 001

I. AUTORIZACIONES

Elaboró:	*Revisó:*	*Autorizó:*
Ing. Salvador Santiago Araujo *Gerente Administrativo*	*Lic. Irais Dafne Mendoza Sánchez* *Director General Adjunto*	*C.P. Jerónimo Javier Mendoza Lara / Lic. Irais Dafne Mendoza Sánchez* *Director General / Director General Adjunto*

Última revisión: Octubre 2025

No. de versión: 11

Fecha de emisión: Noviembre 2014

Revisó: DGE

Aprobó: DGE

INDICE

CONTENIDO
PÁGINA

II. HISTORIAL DE CAMBIOS

Versión	Descripción de Cambios	Autor	Fecha Cambio
1	Versión inicial.	MBS	Noviembre 2014
2	Se agregan referencias	MBS	Agosto 2015
3	Adecuación al contexto de la Organización. Actualización en apartado 4.2 respecto a nuevas partes interesadas identificadas. Adecuación en el alcance del SGSI 4.3. Adecuación en 7.4 apartado de comunicación indicando la forma en que se lleva a cabo ésta. Actualización en 9.1 indicando los elementos a los que se les da seguimiento y medición.	MBS	Diciembre 2015
4	Adecuaciones en 4.2 respecto a las partes interesadas, se acotan los requerimientos de las partes interesadas ya que exceden los requisitos para seguridad de la información. Se quitan como requisitos la Ley Federal de Protección al Consumidor, El Código de Ética para Cobranza de la Asociación de Profesionales de la Cobranza. En 5.3 se anexa matriz de roles y responsabilidades para el SGSI a efecto de hacer más preciso los roles y responsabilidades de los puestos que intervienen la seguridad de la información. Se indica en 9.3 la revisión de las políticas de seguridad de la información como parte de la agenda de la Revisión por la Dirección. Adecuación de 4.3 precisando el alcance de acuerdo al informe de auditoría externo de certificación.	MBS	Junio 2016
5	Adecuaciones en punto 4 del contexto. Se actualiza contexto externo e interno. Se revisaron y analizaron los requisitos de las partes interesadas con los ajustes que se detallan en 4.3 de este documento.	MBS	Enero 2017
6	Actualización en 4.1.2 respecto a la información que se maneja en CIA y que se pretende proteger: se describe más ampliamente lo que se refiere a la información de los empleados, así como en el marco legal y regulatorio. En	MBS	Marzo 2017

Versión	Descripción de Cambios	Autor	Fecha Cambio
	4.2, se incluye la Ley Federal de Protección de Datos Personales para sujetos obligados como parte de los requisitos legales de autoridades regulatorias. En 7.4 se indica la página web de la Organización como mecanismo de comunicación para terceros.		
7	Cambio a nuevo formato, eliminación del contexto de la Organización (se traslada a un documento especifico), sustitución de los procedimientos normativos por los del SGC, alineación de formatos que se tienen en el SGC para hacer menos robustos los Sistemas de Gestión.	MAH	Enero 2018
8	Se actualizó el rubro de "Cuadro de Autorizaciones" con los datos del Coordinador Operativo de TI en lugar del Coordinador de Sistemas de Gestión, así como se actualizó el nombre del nuevo Gerente Administrativo. Se actualizó el alcance del SGSI incluyendo las oficinas de Toluca, así mismo; se actualizó el proceso de Cobranza Especializada como de Cobranza Punta-Punta. Se agregó el apartado de "Abreviaturas y Definiciones" para una mejor comprensión del documento.	RML	Octubre 2020
9	Se eliminó la tabla de "Partes Interesadas" y en su lugar se hace referencia al LIS GSI 009 Matriz de Partes Interesadas del SGSI y se colocó el Mapa General de Procesos en el apartado 4.3 "Determinación del Alcance del SGSI".	JCBH	Junio 2021
10	Se agrego la sección IV – Estructura Organizacional, y se actualizaron los puntos 4.3, 5.2, 5.3, 7.4, 9.2 y 9.3.	SSA	Enero 2022
11	Se realizaron adecuaciones a los puntos 6.1, 6.1.2 y 6.1.3.	SSA	Marzo 2023

III. Abreviaciones y definiciones

Abreviaciones:

DGE	Director General / Director General Adjunto
SGSI	Sistema de Gestión de Seguridad de la Información
GAD	Gerente Administrativo

Definiciones:

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Contexto de la organización: Combinación de cuestiones internas y externas que pueden tener un efecto en el enfoque de la organización para el desarrollo y logro de los objetivos.

Acción correctiva: Acción tomada para eliminar la(s) causa(s) de una no conformidad y evitar que vuelva a ocurrir.

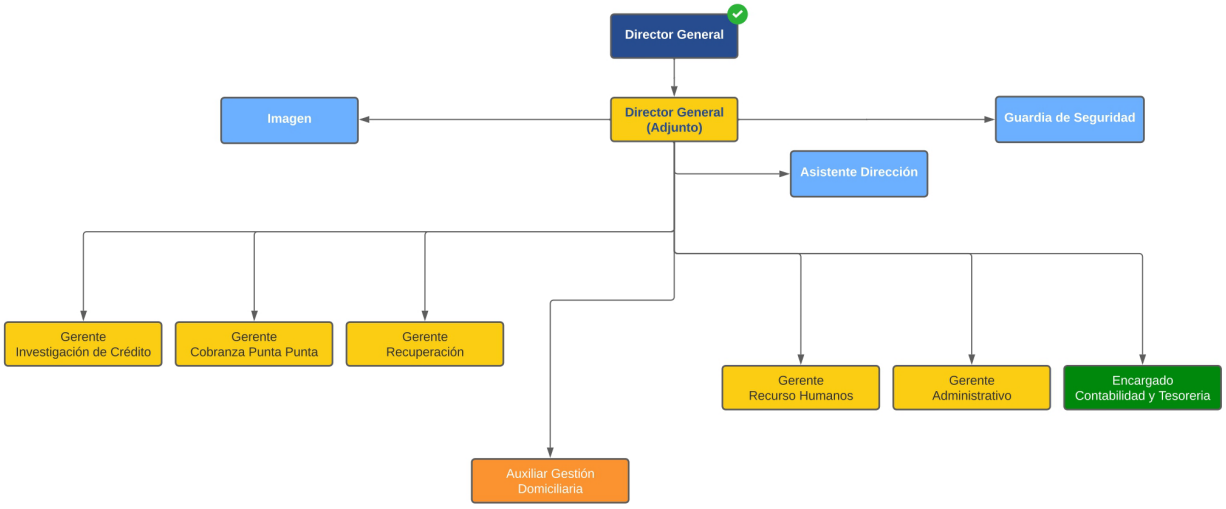
Riesgo: Efecto de la incertidumbre.

Oportunidad de mejora: Posible actividad que no se está realizando, o se realiza de tal modo que podría ser mejorada.

Información documentada: Información que una organización tiene que controlar y mantener, y el medio que la contiene.

IV. Estructura organizacional

ORGANIGRAMA GENERAL



4. CONTEXTO DE LA ORGANIZACIÓN

4.1 COMPRENSIÓN DE LA ORGANIZACIÓN Y DE SU CONTEXTO

Se han determinado las cuestiones externas e internas que son pertinentes para su propósito y dirección estratégica, y que pueden afectar la capacidad para lograr los resultados previstos del SGSI, la información documentada está reflejada en el documento denominado **Contexto de la organización DOC CAL 001**.

4.2 COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

Hemos determinado las partes interesadas relevantes para el Sistema de Gestión de Seguridad de la Información, así como sus requisitos en la **Matriz de Partes Interesadas del SGSI LIS GSI 009**.

4.3 DETERMINACIÓN DEL ALCANCE DEL SGSI

Hemos determinado el alcance del SGSI, considerando el entorno externo e interno y requisitos de las partes interesadas mencionados en los apartados 4.1 y 4.2 del presente manual:

> Para *Consultores e investigadores en administración, S.C:*
> Gestión y administración de cobranza especializada INFONAVIT, Investigación de crédito (referencias comerciales, verificación de propiedades y sociedades en el RPPyC), recuperación de cartera (Extrajudicial y Judicial), cobranza fiscal y gestión domiciliaria.
>
> Para *CIA Integración en Admon, S.R.L, de C.V.:*
> Investigación de Crédito (referencias comerciales, verificación de propiedad y sociedades en el RPPyC) y Gestión Domiciliaria
>
> Para *Aequitas Administradora de Activos, S.R.L. de C. V.:*
> Gestión y administración de cobranza Especializada INFONAVIT y Recuperación de cartera (Extrajudicial y judicial).

Los cuales afectan a los procesos declarados en ***Diagrama de Identificación e Interacción de Procesos (DIIP) PRO-RED-001***

Se declara que todos los puestos de los organigramas de las diferentes áreas que conforman a la organización están dentro del alcance del SGSI. Asimismo, se excluyen a las personas que tengan menos de 90 días dentro de la organización, lo anterior por motivo del periodo de adaptación a la empresa y de una incorporación a la cultura de calidad y seguridad de la información en su totalidad.

Cabe resaltar que la alta dirección ha determinado la creación de dos razones sociales más, por lo que el presente Sistema de Gestión de Seguridad de la Información contempla dentro de su alcance a las empresas siguientes: Consultores e Investigadores en Administración S.C, CIA Integración de Admon S de RL de CV, Aequitas Administradora de Activos S de RL de CV, que en adelante nos referiremos no a una en específico sino a la organización en general, ya que las tres comparten documentación, formatos y personal.

El alcance mencionado aplica para las siguientes sucursales

- **Oficina Nezahualcóyotl:** Av. Lago de Xochimilco No. 283, Col. Ampliación Vicente Villada, Municipio Ciudad Nezahualcóyotl, Estado de México, C.P. 57760.
- **Oficina del Valle:** Insurgentes Sur No. 686 Piso 9, Col. Del Valle, Delegación Benito Juárez, Ciudad de México, C.P. 03100.
- **Oficina Toluca:** Hermenegildo Galeana No. 204, Despacho 2, Col. Centro, Municipio Toluca, Estado de México, C.P. 50000.

El alcance del SGSI también incluye a los siguientes procesos de apoyo.

- Sistemas.
- Recursos Humanos.
- Compras.
- Contabilidad y Tesorería.

Los procesos que se desempeñan por razón social son los siguientes:

Sucursal	Investigación de Crédito	Recuperación de Cartera	Cobranza Punta - Punta	Gestión Domiciliaria	Procesos de Apoyo
Consultores e Investigadores en Administración S.C.	X	X	X	X	X
CIA Integración en Admon S. de R.L. de C.V.	X			X	X
Aequitas Administradora de Activos S. de R.L. de C.V.		X	X		X

4.4 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Hemos establecido (a través de reuniones y acuerdos, así como de una planificación), documentado (en procedimientos, manuales, mapas de proceso, formatos, registros, diagramas, listados, políticas, programas, objetivos, entre otros), implementado (a través de capacitaciones, reuniones, sensibilizaciones, comunicados), y mantenido (con la apreciación del riesgo, controles, plan de tratamiento del riesgo, control de incidentes, auditorías al SGSI, acciones correctivas, revisiones por la Dirección, medición y seguimiento de los procesos, cumplimiento de objetivos y política de seguridad de la información) un Sistema de Gestión de Seguridad de la Información y se mejora continuamente su eficacia por medio de planes de tratamiento, acciones correctivas y planes de cambios y mejoras, de acuerdo con los requisitos de la norma internacional UNE-ISO/IEC 27001:2013.

5. LIDERAZGO

5.1 LIDERAZGO Y COMPROMISO

La alta dirección demuestra su liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información de acuerdo a lo mencionado en el **Instructivo de Responsabilidad de la Dirección INS DIR 001**.

5.2 POLÍTICA

La alta dirección ha establecido una **Política del Sistema de Gestión de Seguridad de la Información POL SGSI 001** que:

a) Es adecuada al propósito de la organización.

b) Proporciona un marco de referencia para el establecimiento de los objetivos de seguridad de la información.

c) incluye el compromiso de cumplir con los requisitos aplicables a la seguridad de la información.

d) Incluye el compromiso de mejora continua del sistema de gestión de seguridad de la información.

La política de seguridad de la información:

a) Está disponible como información documentada en el presente documento, en la página de los sistemas de gestión para fácil acceso de todos los colaboradores de la organización, y en la página web de la organización para consulta de nuestras demás partes interesadas.

b) Es comunicada dentro de la organización por medio comunicados, capacitaciones, presentaciones y boletines mensuales.

c) Está disponible para las terceras partes interesadas en la página web.

Las políticas de seguridad de la información POL GSI 001 son revisadas anualmente o en cuanto se produzcan cambios significativos, según lo indicado en nuestro Manual de gestión de seguridad de la información.

5.3 ROLES, RESPONSABILIDADES Y AUTORIDADES EN LA ORGANIZACIÓN

Se declara respecto a las responsabilidades y autoridad para el SGSI que se cuenta con organigramas y la **Matriz de asignación de roles y responsabilidades FOR GSI 043**, adicional se cuenta con la **Matriz de roles por activos de información críticos FOR GSI 025** y **Carta Responsiva FOR GSI 031**, la cual es derivada de los controles aceptados del **anexo A** y están disponibles y son comunicadas a todos los colaboradores.

La alta dirección asigna responsabilidades y autoridad al:

- Gerente administrativo.
- Coordinador de sistemas de gestión.
- Coordinador de sistemas TI.

Para asegurarse que el sistema de gestión de seguridad de la información es conforme con los requisitos de la norma **UNE EN ISO/IEC 27001:2013** y estos deberán informar a la dirección general el desempeño del sistema de gestión de seguridad de la información.

6. PLANIFICACIÓN

6.1 ACCIONES PARA TRATAR LOS RIESGOS Y OPORTUNIDADES

6.1.1 CONSIDERACIONES GENERALES

En la planificación del SGSI se ha considerado el contexto interno y externo de acuerdo a la naturaleza de nuestros procesos, los requisitos de las partes interesadas, el alcance (descritos en el apartado 4 de este documento) y determina con todo ello los riesgos y oportunidades que son necesarios tratar con el fin de:

a) Asegurar que el SGSI consigue los resultados previstos.
b) Prevenir o reducir efectos indeseados.
c) Lograr la mejora continua del SGSI.

Así mismo planificamos las acciones para tratar los riesgos y oportunidades identificados, también la manera de integrar e implementar las acciones en los procesos del SGSI y evaluar la eficacia de estas acciones.

6.1.2 APRECIACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Definimos y aplicamos un proceso de apreciación de riesgos de seguridad de la información que:

a) Establece y mantiene criterios sobre riesgos de seguridad de la información en el **Procedimiento para el Tratamiento de Riesgos y Oportunidades del SGC y SGSI PRO CAL 009**, incluyendo los criterios de aceptación del riesgo y los criterios para llevar a cabo las apreciaciones de los riesgos de seguridad de la información.

b) Asegura que las sucesivas apreciaciones de los riesgos de seguridad de la información generan resultados consistentes, válidos y comparables.

c) Identifica los riesgos de seguridad de la información asociados a la perdida de confidencialidad, integridad y disponibilidad de la información de acuerdo al alcance del SGSI. Asimismo, identifica a los dueños de los riesgos.

d) Analiza los riesgos de la seguridad de la información, valorando las posibles consecuencias que resultarían si los riesgos identificados llegan a materializarse, valorando de forma realista la probabilidad de los riesgos identificados y determinando los niveles de riesgo.

e) Evalúa los riesgos de seguridad de la información mediante la comparación de los resultados del análisis de riesgo contra los criterios de riesgo establecidos en el apartado 6.1.2 inciso a) de este documento, y priorizando el tratamiento de los riesgos analizados.

6.1.3 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Definimos y efectuamos el **Procedimiento para el Tratamiento de Riesgos y Oportunidades del SGC y SGSI PRO CAL 009**:

a) Seleccionar las opciones adecuadas de tratamiento de riesgo de seguridad de la información teniendo en cuenta los resultados de la apreciación del riesgo.

b) Determinar todos los controles que ha considerado necesarios para implementar las opciones elegidas para el tratamiento del riesgo de seguridad de la información.

c) Comparar los controles determinados a través del documento **Declaración de Aplicabilidad (SOA) LIS GSI 007** y comprobar que no se ha omitido algún control necesario de acuerdo al contexto y alcance del SGSI.

d) Elaborar una **Declaración de Aplicabilidad (SOA) LIS GSI 007** que contiene los controles necesarios y la justificación de las inclusiones y la justificación de las exclusiones de los controles indicados en el **Anexo A** de la norma **UNE-ISO/IEC 27001:2013**.

e) Obtener la aprobación del **Procedimiento para el Tratamiento de Riesgos y Oportunidades del SGC y SGSI PRO CAL 009** y la aceptación de los riesgos residuales de seguridad de la información por parte de los dueños de los riesgos.

Se mantiene información documentada de acuerdo al **Procedimiento para el Tratamiento de Riesgos y Oportunidades del SGC y SGSI PRO CAL 009** sobre el proceso de tratamiento de riesgos de la seguridad de la información.

6.2 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANIFICACIÓN PARA SU CONSECUCIÓN

Hemos establecido los siguientes **Objetivos de Seguridad de la Información FOR CAL 003** en las funciones y niveles pertinentes de la organización:

1. **Controlar el número de incidentes críticos** que afecten la confidencialidad, disponibilidad o integridad de la información.
2. **Mantener la mejora continua** a través de la concientización permanente, implementación de proyectos o adquisición de nueva tecnología.
3. **Reducir el riesgo residual** de manera semestral de acuerdo a la apreciación y tratamiento de los riesgos de la organización**.**

Al planificar cómo lograr los **Objetivos de Seguridad de la Información FOR CAL 003**, la alta dirección y los responsables de las áreas han determinado:

a) Qué se va a medir.

b) Qué recursos se requieren.

c) Quién es el responsable de la medición.

d) Cómo se evaluarán los resultados.

7. SOPORTE

7.1 RECURSOS

La organización determina y proporciona los recursos necesarios tanto humanos, de infraestructura y financieros para el **establecimiento** (a través de reuniones y acuerdos, así como de una planificación), **implementación** (a través de capacitaciones, reuniones, sensibilizaciones, comunicados), **mantenimiento** y **mejora continua** del sistema de gestión de seguridad de la información (con la apreciación del riesgo, controles, planes de acción del riesgo, auditorías al SGSI, acciones correctivas/preventivas, revisiones por la dirección, medición y seguimiento de los procesos, cumplimiento de objetivos y política de seguridad de la información).

7.2 COMPETENCIA

La Organización:

a) Determina la competencia requerida a su personal en materia de seguridad de la información, documentándolo en la **Descripción de puesto FOR REH 001**.

b) Se detectan las necesidades de capacitación, las cuales se van depurando y concentrando en el **Programa Anual de Capacitación**, como se describe en el **Mapa de proceso de Recursos Humanos MAP REH 001**.

c) Cuando es aplicable se ponen en marcha acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones llevadas a cabo de acuerdo al proceso de recursos humanos, pudiendo incluir la formación, la tutoría o la reasignación de las personas empleadas actualmente; o la contratación de personas competentes cuando el puesto así lo requiera.

d) Mantiene los registros apropiados de la competencia de su personal; el área de recursos humanos es responsable de controlar los registros del personal generados durante el transcurso de la relación laboral, esta actividad se encuentra descrita en el **Mapa de proceso de Recursos Humanos MAP REH 001**.

7.3 CONCIENCIACIÓN

Las personas que trabajan en la Organización son concientizadas a través de diferentes herramientas sobre:

a) La política de la seguridad de la información, ya que les ha sido comunicada, explicada a través de capacitación y reuniones.

b) Su contribución a la eficacia del sistema de gestión de seguridad de la información, incluyendo los beneficios de una mejora del desempeño en seguridad de la información; siendo tangible a través de la revisión, al cumplimiento de los objetivos de seguridad de la información y al cumplimiento de los indicadores asociados a los objetivos.

c) Las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información, estás implicaciones se encuentran indicadas en **Código de convivencia**, en las cartas y convenios de confidencialidad, entre otros.

7.4 COMUNICACIÓN

Hemos determinado la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de seguridad de la información, por lo que contamos con un directorio interno publicado en la página de los sistemas de gestión, directorio de proveedores de servicios ti y en el caso de terceros, se cuenta con la página web de la organización en la cual se publica y difunde la política de seguridad de la información, asimismo; en la **Matriz de comunicación FOR CAL 006** se ha determinado el contenido de la comunicación, cuándo comunicar, a quién comunicar, quién debe de comunicar y los procesos por los que debe efectuarse la comunicación.

7.5 INFORMACIÓN DOCUMENTADA

7.5.1 CONSIDERACIONES GENERALES

El Sistema de Gestión de Seguridad de la Información incluye:

a) La información documentada requerida por esta norma internacional y que incluye:
   1. La **Declaración de Aplicabilidad (SOA) LIS GSI 007**,
   2. La **Política de Seguridad de la Información**,
   3. La Apreciación del Riesgo (indicada en la **Matriz de riesgos y oportunidades del SGC y SGSI FOR CAL 016**),
   4. El Alcance del SGSI indicado en este mismo documento,
   5. El Tratamiento del riesgo (**Plan de tratamiento de riesgos y oportunidades del SGC y SGSI FOR CAL 017**).
   6. Los **Objetivos de Seguridad de la Información LIS GSI 003**
   7. La competencia del personal, indicada en la **Descripción de puesto FOR REH 001**, así como evidencia de su cumplimiento en los:
      i. Expedientes del personal,
      ii. Registros de capacitaciones y evaluación de competencias.
   8. Evidencia del análisis, seguimiento, medición, y evaluación a través de
      i. Matriz de Riesgos,
      ii. Apreciación y Tratamiento del riesgo,
      iii. Plan de tratamiento de riesgos.
   9. Evidencia de la planificación de auditorías internas, así como del Informe de la misma.

10. Evidencia de la Revisión por la Dirección.
11. Evidencia de la mejora.

b) Documentos (políticas, procedimientos, listados, controles y formatos) necesarios para asegurarse de la eficaz planificación, desarrollo y control del SGSI.

7.5.2 CREACIÓN Y ACTUALIZACIÓN Y 7.5.3 CONTROL DE LA INFORMACIÓN DOCUMENTADA

Se establece un procedimiento documentado denominado **Control de Información Documentada PRO CAL 001,** en el cual se define los controles necesarios para:

a) La identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);

b) El formato y sus medios de soporte;

c) La revisión y aprobación con respecto a la idoneidad y adecuación.

d) Está disponible y preparada para su uso, dónde y cuándo se necesite;

e) Esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado, o pérdida de integridad).

f) Distribución, acceso, recuperación y uso;

g) Almacenamiento y preservación, incluida la preservación de la legibilidad;

h) Control de cambios (Ver **Lista de información documentada controlada LIS GSI 005**);

i) Retención y disposición.

La información documentada de origen externo, que la Organización ha determinado que es necesaria para la planificación y operación del Sistema de Gestión de Seguridad de la Información, se identifica y controla, según sea adecuado (Ver **Lista de Información documentada externa controlada LIS CAL 002**).

8. OPERACIÓN

8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL

La organización planifica, implementa y controla los procesos necesarios para cumplir los requisitos de seguridad de la información y para implementar las acciones determinadas en el apartado 6.1 de este documento.

También planes para alcanzar los **Objetivos de seguridad de la información FOR CAL 003**, los cuales se documentan según aplique.

Mantiene información documentada, para tener la confianza de que los procesos se han llevado a cabo según lo planificado, se controlan los cambios planificados (los cuales se llevan a cabo mediante proyectos) y revisa las consecuencias de los cambios no previstos, llevando a cabo acciones para mitigar los efectos adversos, cuando sea necesario.

Cuando sea pertinente se documentará en un **Plan de cambios y mejoras FOR CAL 011**.

8.2 APRECIACIÓN DE LOS RIESGOS DE SEGURIDAD DE INFORMACIÓN

Llevamos a cabo la apreciación de riesgos de seguridad de la información a intervalos planificados (semestralmente, y cuando se propongan o se produzcan modificaciones importantes, teniendo en cuenta los criterios establecidos en el punto 6.1.2 a) de este documento.

Se conserva información documentada de los resultados de las apreciaciones de riesgos de seguridad de información.

8.3 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE INFORMACIÓN

Se implementa el **Plan de tratamiento de riesgos y oportunidades del SGC y SGSI FOR CAL 017** con base en la **Matriz de riesgos y oportunidades del SGC y SGSI FOR CAL 016.**

Se conserva información documentada de los resultados del tratamiento de los riesgos de seguridad de información.

9. EVALUACIÓN DEL DESEMPEÑO

9.1 SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

Se evalúa el desempeño de la seguridad de la información y la eficacia del Sistema de Gestión de Seguridad de la Información mediante los siguientes mecanismos de medición y seguimiento:

a) Incidentes de seguridad de la información y su tratamiento.

b) Seguimiento y cierre de los hallazgos de auditoría interna y externa realizados al SGSI.

c) Apreciación del riesgo (análisis, evaluación).

d) Tratamiento del riesgo identificado mediante la apreciación.

e) Medición y seguimiento de los objetivos de seguridad de la Información.

De todo lo anterior conservamos información documentada adecuada como evidencia de los resultados.

9.2 AUDITORÍA INTERNA

Nuestra empresa lleva a cabo auditorías internas a intervalos planificados de acuerdo al **Calendario de auditorías FOR CAL 014**, para proporcionar información acerca del sistema de gestión de seguridad de la información:

a) Cumple con:
   1. Los requisitos propios de la organización para su sistema de gestión de seguridad de la información.
   2. Los requisitos de **UNE-ISO/IEC 27001:2013.**

b) Está implementado y mantenido de manera eficaz.

En el **Calendario de auditorías FOR CAL 014** se programan las auditorías internas, tomando en consideración la importancia de los procesos y los resultados de auditorías anteriores, así como la selección de auditores, la objetividad e imparcialidad del proceso de auditoría, así como los criterios, el alcance y la metodología de la auditoría interna los cuales quedan definidos en el **Procedimiento de Auditorías Internas PRO CAL 003**.

El equipo auditor seleccionado tiene la responsabilidad de asegurar la objetividad e imparcialidad (en medida de lo posible) del proceso de auditoria siguiendo el **Procedimiento de Auditorías Internas PRO CAL 003** establecido por la organización y asegurándose que los auditores no auditan su propio trabajo.

El procedimiento documentado incluye las responsabilidades, los requisitos para la planificación y realización de auditorías, la forma como se comunican los resultados y de qué modo se mantienen los registros, las actividades de seguimiento y medición incluyen las acciones tomadas y el informe de resultados de la verificación.

9.3 REVISIÓN POR LA DIRECCIÓN

La alta dirección revisa el sistema de gestión de seguridad de la información de la organización a intervalos planificados en el **Calendario de Revisión por Dirección FOR CAL 005**, para asegurarse de su conveniencia, adecuación y eficacia continuas de acuerdo con lo establecido en el **Instructivo de Responsabilidad de la Dirección INS DIR 001**.

La revisión por la dirección incluye consideraciones sobre:

a) El estado de las acciones desde anteriores revisiones por la dirección.

b) Los cambios en las cuestiones externas e internas que sean pertinentes al Sistema de Gestión de Seguridad de Información.

c) La información sobre el comportamiento de la seguridad de información, incluidas las tendencias relativas a:

   1. No conformidades y acciones correctivas.
   2. Seguimiento y resultados de las mediciones.
   3. Resultados de auditoría.
   4. El cumplimiento de los objetivos de seguridad de la información.

d) Los comentarios provenientes de las partes interesadas.

e) Los resultados de la apreciación del riesgo y el estado del plan de tratamiento de riesgos.

f) Las oportunidades de mejora continua.

g) La revisión de las políticas de seguridad de la información.

Los elementos de salida de la revisión por la dirección incluyen las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de gestión de seguridad de la información.
Se mantienen registros de las revisiones en la **Minuta de Revisión por Dirección FOR DIR 008.**

10. MEJORA

10.1 NO CONFORMIDAD Y ACCIONES CORRECTIVAS

Cuando ocurre una no conformidad se lleva a cabo lo establecido en el **Procedimiento de Acciones correctivas PRO CAL 002**.

a) Reacciona ante la no conformidad, y según sea aplicable:

   1. Lleva a cabo acciones para controlarla y corregirla, y

   2. Hacer frente a las consecuencias,

b) Evalúa la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir, ni ocurra en otra parte, mediante:

   1. La revisión de la no conformidad,

   2. La determinación de las causas de la no conformidad, y

   3. La determinación de si existen no conformidades similares, o que potencialmente podrían ocurrir;

c) Implementa cualquier acción necesaria;

d) Revisa la eficacia de las acciones correctivas llevadas a cabo; y

e) Si es necesario, hace cambios al Sistema de Gestión de Seguridad de la Información.

Las acciones correctivas son adecuadas a los efectos de las no conformidades encontradas.

Se conserva evidencia de:

f) La naturaleza de las no conformidades y cualquier acción posterior llevada a cabo; y

g) Los resultados de cualquier acción correctiva.

10.2 MEJORA CONTINUA

La organización mejora de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de la información mediante el uso de la política de seguridad de la información, los objetivos de seguridad de la información y su cumplimiento, los resultados de las auditorías internas y externas, la apreciación y el tratamiento del riesgo, las acciones correctivas, la revisión por la dirección, los controles establecidos para evitar y/o mitigar el riesgo, entre otros.

Cuando sea pertinente se documentará en un **Plan de cambios y mejoras FOR CAL 011**.