



PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

	Cargo	Nombre
Elaborado por:	Oficial de Seguridad de la Información y Protección de Datos Personales y Abiertos	Jenny Castañeda Zubiaur
Revisado por:	Gerente de Planeamiento y Presupuesto	David Villavicencio Fernández
	Gerente de Asesoría Legal	Alberto Arequipaño Tamara
Aprobado por:	Gerente General (e)	David Villavicencio Fernández



Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**



	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: Página	05 2 de 13

TABLA DE CONTENIDO

CONTROL DE CAMBIOS	3
1. OBJETIVO:.....	4
2. ALCANCE:	4
3. RESPONSABLE(S):.....	4
4. BASE LEGAL:	4
5. DOCUMENTOS DE REFERENCIA.....	4
6. DEFINICIONES Y ABREVIATURAS:.....	4
7. DISPOSICIONES GENERALES.....	5
8. DESCRIPCIÓN	7
9. REGISTROS	9
10. ANEXOS	9



Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**


	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: Página	05 3 de 13

CONTROL DE CAMBIOS

N° Versión	Fecha	Descripción del cambio	Responsable del Documento
04	22/10/2019	<p>Se realizaron los siguientes cambios:</p> <ul style="list-style-type: none"> a) Se ha incluido las versiones actualizadas de los documentos referenciados y las nuevas normativas aplicables al SGSI. b) Se actualizó la estructura del documento de acuerdo a lo normado en la versión vigente del procedimiento P-SGSI-03 – “Control de Información Documentada”. c) Se incluyó la sección de “Consideraciones Generales” donde se establece criterios que se aplican a todo el procedimiento, incluyendo la información de clasificación de incidentes y tiempos de respuesta. d) Se actualizó las siglas de los formatos de acuerdo al procedimiento P-SGSI-03 – “Control de Información Documentada”. e) Se incluyó el formato de atención de incidentes de seguridad de la información. f) Se incluyó el formato de Base de Conocimientos de Incidentes de Seguridad de la Información. 	Oficial de Seguridad de la Información y Protección de Datos Personales y Abiertos
05	23/11/2020	<p>Se realizaron los siguientes cambios:</p> <ul style="list-style-type: none"> a) Se actualizó la estructura del documento de acuerdo a lo normado en la versión vigente del procedimiento PR-SGSI-003 – “Control de Información Documentada”. b) Se precisa en disposiciones generales, las fuentes de entrada para la notificación o reporte de incidentes. c) Se incluye en la descripción del procedimiento lo relacionado a las nuevas fuentes de entrada de notificación o reporte. 	Oficial de Seguridad de la Información y Protección de Datos Personales y Abiertos



Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**

	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión:	05
		Página	4 de 13

1. Objetivo:

El objetivo del presente documento es establecer las actividades a seguir para la notificación, clasificación, asignación para el tratamiento y cierre de los incidentes de seguridad de la información del Sistema de Gestión de Seguridad de la Información (SGSI).

2. Alcance:

Este documento se aplica a todo el Sistema de Gestión de Seguridad de la Información (SGSI) y los usuarios son las unidades orgánicas involucradas en los procesos del SGSI.

3. Responsable(s):

Oficial de Seguridad de la Información y Protección de Datos Personales y Abiertos.

4. Base Legal:

- 4.1. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- 4.2. Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición".

5. Documentos de referencia

- 5.1 Norma ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.
- 5.2 Procedimiento PR-SGSI-003 - "Control de Información Documentada".


6. Definiciones y Abreviaturas:

6.1. Definiciones

Base de Conocimiento:	Repositorio de información centralizado que permite compartir conocimiento e información dentro de la organización. El propósito primordial de esta gestión es mejorar reduciendo la necesidad de redescubrir conocimientos.
Evento de seguridad de la información:	Ocurrencia identificada en un sistema, servicio o red indicando una posible brecha de la política de seguridad de la información o falla de las salvaguardas o una situación desconocida previa que puede ser relevante.
Incidente de la seguridad de la información:	Una serie de eventos no deseados que tienen una probabilidad significativa de comprometer operaciones del negocio y amenazar la seguridad de la información.

Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**



	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión:	05
		Página	5 de 13

Personal Involucrado	Se considera así a los responsables de la UO, personal que administra la herramienta tecnología posiblemente afectada en el evento.
Reportante	Colaborador o tercero, personal de seguridad física, responsables de la administración y operación de tecnologías de la información, personal de soporte técnico, entidades rectoras (PCM, SeGDi), proveedores, personas o entidades externas.

6.2. Abreviaturas

CGD	Comité de Gobierno Digital del OSIPTTEL
CISO	Oficial de Seguridad de la Información y Protección de Datos Personales y Abiertos
GG	Gerencia General
PCM	Presidencia del Consejo de Ministros
SeGDi	Secretaría de Gobierno Digital
SGSI	Sistema de Gestión de Seguridad de la Información
UO	Unidad Orgánica


7. Disposiciones Generales

- 7.1. Todo colaborador o tercero del OSIPTTEL esté o no involucrado en el SGSI tienen la responsabilidad de reportar cualquier evento o incidente de seguridad de la información que haya detectado.
- 7.2. Las fuentes de reporte o detección, además de los colaboradores, son el personal de seguridad física, los responsables de la administración y operación de tecnologías de la información, personal de soporte técnico, entidades rectoras (PCM, SeGDi), proveedores, herramientas de monitoreo y/o seguridad informática y personas o entidades externas.
- 7.3. Los eventos reportados posterior a su evaluación pueden ser catalogados como incidentes de seguridad de la información, mantenerse como eventos de seguridad o desestimarse por deberse algún error.
- 7.4. Todo el equipamiento informático debe encontrarse sincronizado en fecha y hora para lo cual deberán usar una misma fuente horaria.
- 7.5. La criticidad del incidente será evaluado de acuerdo a los niveles de impacto de la metodología de Gestión de Riesgos:

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Las consecuencias tienen efectos mínimos sobre la entidad.
2	Menor	Las consecuencias tienen bajo impacto o efecto sobre la entidad.
3	Dañino	Las consecuencias tienen mediano impacto o efecto sobre la entidad.

Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**



	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: Página	05 6 de 13

4	Severo	Las consecuencias tienen alto impacto o efecto sobre la entidad
5	Crítico	Las consecuencias tienen desastroso impacto o efecto sobre la entidad


- 7.6. El tiempo de respuesta establecido en la siguiente tabla es aproximado al tiempo máximo para que el incidente sea atendido dependiendo del nivel del impacto, y no corresponde al tiempo de solución del incidente, dado que la complejidad de la atención varía dependiendo del tipo de incidente y del activo de información impactado.

NIVEL DEL IMPACTO	TIEMPO DE RESPUESTA
Insignificante	3 horas
Menor	1 hora
Dañino	30 minutos
Severo	15 minutos
Crítico	10 minutos

- 7.7. Los colaboradores involucrados en el análisis del evento de seguridad o su tratamiento deben de facilitar la información requerida al CISO para su correspondiente evaluación.



Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**


	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: Página	05 7 de 13

8. Descripción

UO	Ejecutor	Actividad		Producto(s)
		N°	Descripción	
			<p>Inicio</p> <p>Si inicia por el colaborador: ir a la actividad 1</p> <p>Si es alerta automática: ir a la actividad 2</p>	
UOU	Reportante	1.	<p>Reportar el evento de seguridad de la Información de forma inmediata a la detección detallando la mayor información que le sea posible, mediante uno de los siguientes medios:</p> <ul style="list-style-type: none"> a. Correo electrónico a informacionsegura@osiptel.gob.pe o b. Llamada al Teléfono: 2251313 Anexo 2483 o al 961271458 <p>En caso de que el reportante sea el SeGDi (PCM) Se comunica a la cuenta de correo o número telefónico personal del CISO, por llamada telefónica o mensaje electrónico.</p>	<p>Mensaje electrónico o Llamada Telefónica con reporte de alerta</p>
GG	CISO	2.	<p>Analizar el evento y solicitar información a las UO involucradas o al reportante para poder evaluar.</p>	<p>Mensaje electrónico solicitando información adicional</p>
UOU	Personal involucrado o Reportante	3.	<p>Remitir la información complementaria al CISO para su evaluación.</p> <p>En caso de que el reportante sea el SeGDi (PCM) Se comunica a la cuenta de correo o número telefónico personal del CISO, por llamada telefónica o mensaje electrónico.</p>	<p>Mensaje electrónico al CISO con información complementaria</p>
GG	CISO	4.	<p>Revisar la información complementaria y validar que corresponde a un evento real y no un error del reportante o la herramienta.</p> <p>Si se reportó un evento real: ir a la actividad 6. Caso contrario (Si es error): ir a la actividad 5</p>	<p>Información complementaria validada</p>
GG	CISO	5.	<p>Comunicar al reportante, vía correo electrónico, que lo reportado no corresponde a un evento de seguridad de la información.</p> <p>Fin del procedimiento.</p>	<p>Correo electrónico cerrando el reporte.</p>
GG	CISO	6.	<p>Evaluar si el evento llega a ser catalogado como incidente de seguridad de la información.</p> <p>Si es incidente: ir a la actividad 9. Caso contrario: ir a la actividad 7.</p>	<p>Evento catalogado</p>

Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**




	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión:	05
		Página	8 de 13

UO	Ejecutor	Actividad		Producto(s)
		Nº	Descripción	
GG	CISO	7.	Comunicar a la UO responsable de gestionar el evento y solicitar responder con las acciones realizadas.	Correo electrónico indicando a la UO realizar acciones
UOU	Responsable de UOU	8.	Remitir, vía correo electrónico, al CISO detalle de acciones realizadas. Fin del procedimiento	Correo electrónico con acciones realizadas
GG	CISO	9.	Clasificar el incidente tomando en cuenta lo especificado en el ítem 7.5 sobre su impacto y registrar la información en el Anexo 02: PR-SGSI-001-F-001 – “Formato de atención de incidentes de seguridad de la información”.	Anexo 02 con información inicial registrada
GG	CISO	10.	Comunicar, por correo electrónico, el incidente al personal responsable de darle tratamiento y solicitar su atención de acuerdo a los niveles de prioridad y tiempos de respuesta.	Correo electrónico encomendando al personal responsable el tratamiento al incidente
UOU	Responsable(s) de las acciones de tratamiento	11.	Dar tratamiento al incidente de acuerdo a la clasificación de los activos involucrados y de su impacto, considerando los tiempos de respuesta establecidos para su resolución. Las acciones a ejecutar son coordinadas con todos los involucrados.	Correos electrónicos de coordinación
UOU	Responsable(s) de las acciones de tratamiento	12.	Registrar las acciones realizadas en el Anexo 02: formato PR-SGSI-001-F001 con un nivel de detalle que permita usar dicha información frente a incidentes similares y comunicar, vía correo electrónico, al CISO sobre la culminación de su atención.	Anexo 02 con acciones realizadas registradas
GG	CISO	13.	Verificar la resolución del incidente junto con el propietario del activo involucrado.	Resolución del incidente conjuntamente verificado
GG	CISO	14.	Registrar la información en el Anexo 02: formato PR-SGSI-001-F-001, cerrando el incidente.	Anexo 02 completo
GG	CISO	15.	Comunicar al propietario del activo(s) involucrado(s) y al reportante sobre la finalización de la atención del incidente y su correspondiente cierre.	Correo electrónico comunicando el cierre del incidente
GG	CISO	16.	Consolidar toda la información sobre el tratamiento para mantener una base de los conocimientos que sirvan de apoyo ante incidentes futuros y completar el Anexo 03: formato PR-	Anexo 03 completado

Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**



	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión:	05
		Página	9 de 13

UO	Ejecutor	Actividad		Producto(s)
		Nº	Descripción	
			SGSI-001-F-002 – Base de Conocimiento de Incidentes Seguridad de la Información.	
GG	CISO	17.	Reportar, por memorando o mediante una reunión, al CGD sobre el incidente suscitado. Los incidentes deben reportarse, con una frecuencia mínima semestral.	Memorando o Acta de Reunión

9. Registros

CÓDIGO	NOMBRE DEL REGISTRO	UBICACIÓN	RESPONSABLE DE CONSERVACIÓN	TIEMPO DE CONSERVACIÓN
PR-SGSI-001-F-001	Formato de atención de incidentes de seguridad de la información	Unidad W	CISO	Permanente
PR-SGSI-001-F-002	Base de conocimientos de Incidentes Seguridad de la Información	Unidad W	CISO	Permanente

10. Anexos


10.1. Diagrama de flujo

10.2. Formato de atención de incidentes de seguridad de la información

10.3. Formato base de conocimientos de incidentes de seguridad de la información

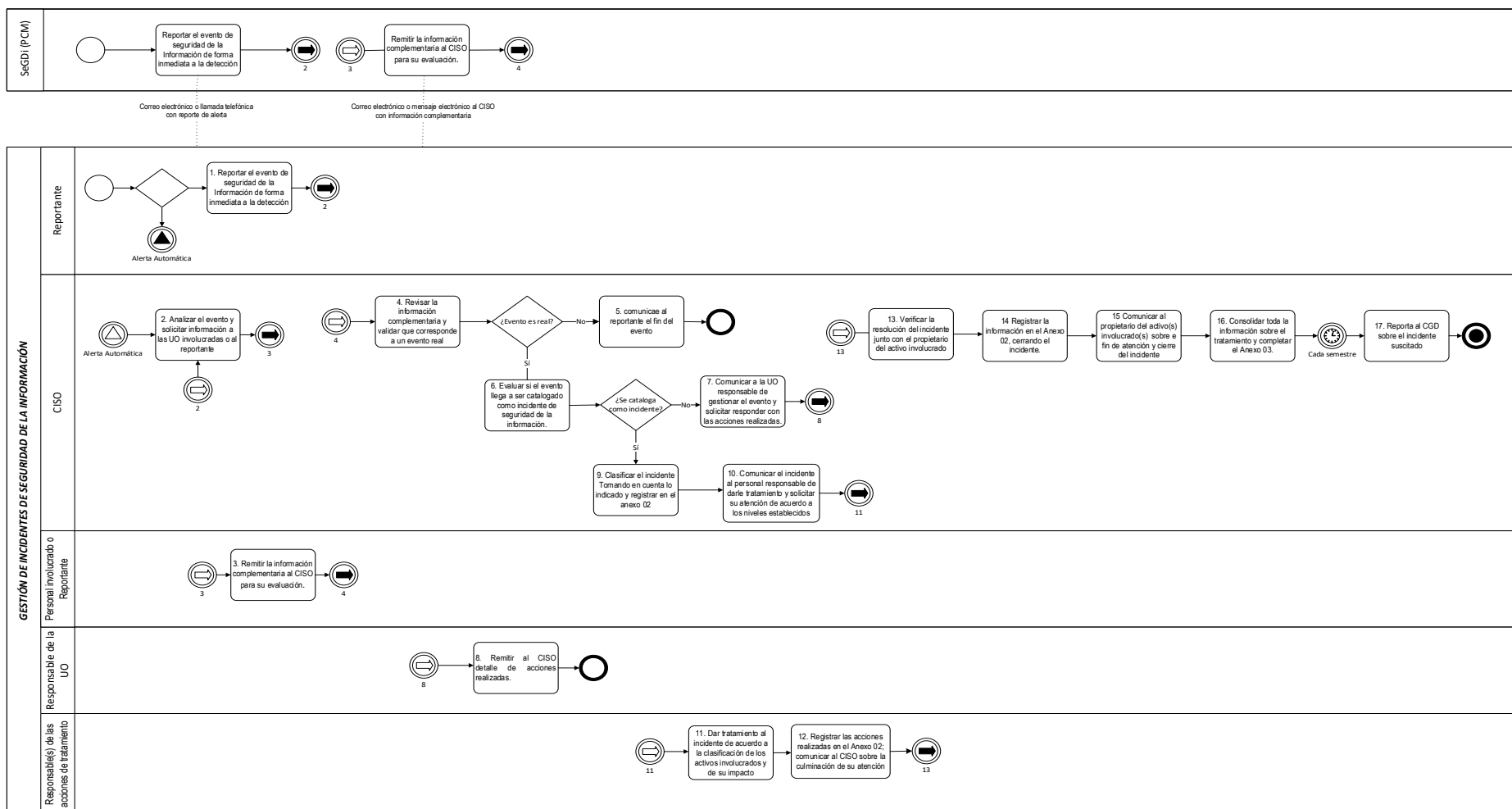


Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**


	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión:	05
		Página	10 de 13

10.1. DIAGRAMA DE FLUJO

10.1.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN



Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**

	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 05 Página 11 de 13	


10.2. Formato de atención de incidentes de seguridad de la información

PR-SGSI-001-F-001

FORMATO ATENCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN					
DATOS DEL REPORTANTE					
NOMBRES Y APELLIDOS		CARGO			
CORREO ELECTRÓNICO		UO			
FECHA Y HORA		N° INCIDENTE			
TIPO DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN					
Acceso lógico no autorizado a servicios y recursos tecnológicos	Pérdida de Información física o de equipamiento que alberga información digital	Ataques de Ingeniería Social			
Acceso físico no autorizado a los recursos e instalaciones	Robo de información física o de equipamiento que alberga información digital	Ataques de denegación de servicio			
Uso inadecuado de la información, recursos y servicios	Destrucción no autorizada de información	Ataques de infección por código malicioso			
Divulgación de información (física/digital) no autorizada	Modificación no autorizada de información, recursos y servicios.	Otros:			
DESCRIPCIÓN DEL INCIDENTE					
ACTIVOS INVOLUCRADOS					
DEBILIDADES IDENTIFICADAS					
FLUJO DE ATENCIÓN					
ATENCIÓN N° 01*					
NOMBRES Y APELLIDOS		CARGO			
FECHA Y HORA INICIO		FECHA Y HORA FIN			
ACCIONES					

Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**



	PROCEDIMIENTO	Código:	PR-SGSI-001
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: Página	05 12 de 13

Aquí se describe las acciones que se han realizado para atender el incidente.

**Pueden insertarse tantas secciones de atención como cantidad de responsables estén involucrados en las acciones.*

CIERRE DEL INCIDENTE	
FECHA Y HORA	
VERIFICADO POR	
MEJORAS IMPLEMENTADAS	
OBSERVACIONES	



Las únicas **COPIAS CONTROLADAS** de los documentos aprobados del SGSI se encuentran publicadas en la Intranet, sección **Sistema de Gestión de la Seguridad de la Información**

