

"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE
SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA
NACIÓN - ETAPA 1"



Suprema Corte
de Justicia de la Nación

CONTRATO: SCJN/DGRM/DPC-014/07/2022

REFERENCIA: 09. DOCUMENTOS DE DISEÑO
DEL SISTEMA INTEGRAL DE SEGURIDAD



GRUPO SIAYEC[®]
— EXPERTOS EN TECNOLOGÍA —



DOCUMENTO MAESTRO



Suprema Corte
de Justicia de la Nación



**Servicio Administrado
para la Solución de
Seguridad de la Suprema
Corte de Justicia de la
Nación - Etapa 1**

**09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE
SEGURIDAD**

 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD



Documento Maestro del Sistema Integral de Seguridad para la Gestión Integral del Riesgo Suprema Corte de Justicia de la Nación

**Basado en las Normas
ISO 9001, ISO 31000, ISO 27001, ISO 20000-1**

 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

CONTENIDO

INTRODUCCIÓN	4
CONTEXTO DEL SISTEMA EN LA SCJN	5
OBJETIVOS DEL SISTEMA	6
OBJETIVOS ESPECÍFICOS	6
ALCANCE	7
DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD.	9
MODELO DEL SISTEMA	16
DECLARACIONES Y EXCLUSIONES	17
ESTRUCTURA DOCUMENTAL	18
APROBACIONES	19
CONTROL DE CAMBIOS	20
DOCUMENTOS DE REFERENCIA	21



 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

INTRODUCCIÓN

El Sistema Integral de Seguridad para la Gestión de Riesgos (SISGR) de la Suprema Corte de Justicia de la Nación, está diseñado para que le proporcione al Edificio Sede de la Institución, una solución integral de seguridad, protección y control, cuyo eje principal sea la generación, procesamiento y análisis de datos, obteniendo información oportuna, actualizada y veraz, que fortalezca la capacidad de prevención y respuesta necesaria en caso de un evento o incidente que ponga en riesgo a las personas.

El SISGR contiene las siguientes secciones:

- a. Sistema Integral de Seguridad para la Gestión del Riesgo, Riesgos identificados, así como el tratamiento de estos para la prevención, respuesta y recuperación.
- b. Sistema de información y base de datos unificada. (SIBDU)
- c. Cuadro de Mando Integral y Solución de Gestión Integral de explotación de información
- d. Protocolos de actuación, manual de procesos y procedimientos técnicos y operativos.
- e. Inteligencia de riesgos

 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

CONTEXTO DEL SISTEMA EN LA SCJN



La Suprema Corte de Justicia de la Nación (SCJN) es el Máximo Tribunal Constitucional del país y cabeza del Poder Judicial de la Federación. Entre sus responsabilidades destacan: defender el orden establecido por la Constitución Política de los Estados Unidos Mexicanos; mantener el equilibrio entre los distintos Poderes y ámbitos de gobierno, así como solucionar asuntos de gran trascendencia para la sociedad

Dirección General de Seguridad (DGS) tiene como función principal dirigir y coordinar los servicios de seguridad en la Suprema Corte de Justicia de la Nación (SCJN), a fin de proteger y defender la integridad de las personas, así como de los bienes muebles e inmuebles de la Institución.

Es importante mencionar que la emisión del presente Manual tiene su razón de ser en el incremento de las capacidades de la infraestructura, el equipamiento y la tecnología del Centro de Control de Seguridad Integral de la Corte (C2SIC) de la SCJN.

Con el manual se pretende consolidar el Sistema Integral de Seguridad y Gestión de Riesgos (SISGR) y, en general al incremento de las capacidades de seguridad de la Dirección General de Seguridad, lo cual permitirá generar información estratégica y productos de inteligencia para prevenir, mitigar y enfrentar riesgos de manera efectiva.

El Manual parte de un modelo de inteligencia de riesgos, el cual se nutre de información proveniente de reportes operativos, incidencia delictiva, intercambio de información con otras instituciones, antecedentes sobre incidentes de vulnerabilidad de la seguridad, análisis de medios de comunicación y redes sociales, con objeto de generar mapas y ponderaciones de riesgos, así como productos de inteligencia para la prevención, mitigación y reacción efectiva ante riesgos.



 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

OBJETIVOS DEL SISTEMA

La Suprema Corte de Justicia de la Nación cuenta con una solución tecnológica de control y videovigilancia que permite llevar a cabo las estrategias de seguridad para minimizar la posibilidad de que algunos riesgos identificados pudieran materializarse, incrementar los niveles de seguridad, mediante soluciones tecnológicas y efectuar acciones de prevención de riesgos de instalaciones, bienes y personas; establecer un mecanismo eficiente y efectivo en tiempo real de seguridad, protección, rastreo y monitoreo, para salvaguardar la integridad física de las personas servidoras públicas, visitantes y la seguridad del inmueble, facilitando la toma oportuna de decisiones y acciones.

OBJETIVOS ESPECÍFICOS

Descripción	Medición	Norma	Responsable
Promover operaciones de Prevención a la Seguridad y Protección Integral, desarrollando acciones de inteligencia de carácter estratégico y de atención, prevención, coordinación y seguimiento a los riesgos y amenazas tanto interno como externo.	Anual en base al estudio de riesgos	ISO 31000	Director General de Seguridad.
Salvaguardar a las personas, los activos físicos, financieros, tecnológicos y de información entre otros.	A través de Key Performance Indicator (KPIs) e Indicadores Clave de Riesgo (KRI)	ISO 9000, ISO 31000, ISO 27001, ISO 20000	Director General de Seguridad. Director General de Servicios Informáticos Recursos Humanos
Establecer un área de inteligencia que produzca análisis estratégico que apoye a la toma de decisiones en materia de seguridad y protección.	Planeación, medición y revisión mensual	ISO 31000	Director General de Seguridad Comité de Riesgos
Determinar un proceso de mejora continua en el análisis de riesgos de todas las instalaciones de la Institución con el objeto de conocer los	Semestral en base a auditorías al Sistema y resultados de los SLA's de los servicios contratados	ISO 9000, ISO 31000, ISO 27001, ISO 20000	Director General de Seguridad Comité de Riesgos

 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

posibles riesgos e implementar medidas de mitigación			
Promover el concepto de cultura en seguridad y protección, para contribuir al conocimiento colectivo y fortalecer la toma de conciencia sobre los principales riesgos y amenazas, así como su posible impacto en la vida de la población de la Institución, de manera inicial en el edificio sede y con las bases para extenderlo a otras sedes.	Evaluaciones de confianza y formación/actualización continua	ISO 9000, ISO 31000,	Director General de Seguridad Comité de Riesgos Recursos Humanos



ALCANCE

El Sistema Integral de Seguridad para la Gestión de Riesgos (SISGR) de la Suprema Corte de Justicia de la Nación, está diseñado con los siguientes procesos que integran el sistema:

- a. Sistema Integral de Seguridad para la Gestión del Riesgo, Riesgos identificados, así como el tratamiento de estos para la prevención, respuesta y recuperación.
- b. Sistema de información y base de datos unificada. (SIBDU)
- c. Cuadro de Mando Integral y Solución de Gestión Integral de explotación de información
- d. Protocolos de actuación, manual de procesos y procedimientos técnicos y operativos.
- e. Inteligencia de riesgos.
- f. Plataforma Tecnológica
- g. Niveles de Servicio y soporte

Estos procesos centrales se apoyan de otros: Recursos Humanos, Presupuestos, Infraestructura que apoyan el desempeño del Sistema.


Como parte de la metodología que marcan las Normas ISO 9000:2015, ISO 20000-1, ISO 27001 e ISO 31000, se integran al SISGR sus respectivos requerimientos traducándose en el siguiente alcance en cuanto a procesos se

 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

requiere, dichos procesos se implementan en base a los referidos e implementados por Grupo Siayec, quedando como referencia para su aplicación, seguimiento y auditoría:


Clasificación	Procesos Identificados	Norma aplicable			
		ISO 9000	ISO 27001	ISO-20000-1	ISO-31000
Procesos Centrales	SCJN-SISGR-01 Gestión de Riesgos	X	X	X	X
	SCJN-SISGR-02 CONOPS	X	X	X	X
	SCJN-SISGR-03 SIBDU	X	X	X	X
	SCJN-SISGR-04 Cuadro de Mando Integral	X	X	X	X
	SCJN-SISGR-05 Protocolos de actuación	X			X
	SCJN-SISGR-06 inteligencia de Riesgos	x			X
Procesos de Apoyo	SCJN-SISGR-07 Plataforma Tecnológica	X	X	X	
	SCJN-SISGR-08 Mantenimiento y Soporte técnico	X	X	X	
	SCJN-SISGR-09 Relación con otros organismos	X	X	X	X

Derivado de los alcances del servicio descrito en el anexo técnico Apéndice G4 Sistema Integral de Seguridad para la Gestión del Riesgo y a los procesos planteados en este Manual, Grupo Siayec hace referencia a los procesos que atienden los requerimientos previstos, cubriendo dentro de su definición y aplicación su cumplimiento, implementación y auditoría, acorde a los planes corporativos la política prevista, a continuación se desglosan y refieren a los anexos de este manual.


	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD.


DOCUMENTO	DOCUMENTO REFERENCIA	Descripción breve del contenido del archivo y la justificación de su creación.
DOCUMENTO MAESTRO DEL SISTEMA INTEGRAL DE SEGURIDAD PARA LA GESTION INTEGRAL DE RIESGO: Documento que contiene la descripción y alcance del Sistema Integral de Seguridad para la Gestión del Riesgo, Riesgos identificados, así como el tratamiento de estos para la prevención, respuesta y recuperación.	MSG ED4 Manual del Sistema de Gestión. PC-10-01 ED1 Seguridad de la Información.	<p>El MSG describe el alcance del sistema de gestión integral, incluye todos los procesos implementados para ISO 9001 Calidad, 20000-1 Servicios de TI e ISO 27001 Seguridad de la Información, así como el contexto de la organización, exclusiones, responsables, partes interesadas, autorizaciones.</p> <p>El Proceso PC-10-01 Seguridad de la Información, incluye varios subprocesos entre estos:</p> <ol style="list-style-type: none"> 1) Las estrategias de seguridad de la información, 2) Hacer la evaluación y tratamiento de los riesgos a la Seguridad de la Información y monitorear que se apliquen las políticas para los procesos Alta, Baja y Cambios de usuarios, Gestionar la continuidad negocio, Respalda la información y Transferir la Información. <p>Todos los procesos sin excepción en su carátula incluyen los requisitos aplicables a cada norma. El proceso de Seguridad de la Información da cumplimiento a 14 requisitos de las tres normas ISO mencionadas.</p>

	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 <p>Suprema Corte de Justicia de la Nación</p>
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD


DOCUMENTO	DOCUMENTO REFERENCIA	Descripción breve del contenido del archivo y la justificación de su creación.
a. Tener procedimientos documentados de gestión de incidentes que aborden las infracciones o la pérdida de confidencialidad.	AT'N. DE INCIDENTES Proceso PC-09-01 ED2 Atención de solicitudes e incidentes	<p>Grupo Siayec cuenta con una herramienta llamada SDP - Service Desk Plus V10 a través de la cual se administra la operación de los tickets y/o Solicitudes de Soporte, así como la Atención de solicitudes de Servicio. También se cuenta con un PRTG (Sistema de monitoreo), considerado como uno de los principales equipos de comunicación. Se cuenta con personal capacitado y especializado en sus diferentes niveles de atención y/o complejidad.</p> <p>Se establecen SLA's de servicios de forma personalizada para la Suprema Corte de Justicia de acuerdo al contrato de referencia. Y de acuerdo a la criticidad y valoración de cada ticket también se atienden los tickets de problemas y de gestión de cambios.</p> <p>Todas las actividades anteriores se describen como parte del Proceso de Atención de Solicitudes e Incidentes atendido por el equipo de ingenieros de la Mesa de Servicios 24x7 los 365 del año.</p> <p>De igual manera en su portada describe 8 de los requisitos aplicables a las normas ISO 9001, 20000-1 Y 27001. Así como documentos de consulta relacionados al proceso, tales como: formato de Pólizas de soporte (SLA's), Formato de Esquema de atención del NOC, Instructivo de Atención de Solicitud e incidentes y Base de datos de conocimiento.</p>
b. Tener procedimientos documentados de gestión de incidentes que aborden la recopilación de pruebas y documentación, así como la protección de la cadena de custodia.	PROCEDIMIENTO (VIDA UTIL DEL TICKET) Proceso PC-09-01 ED2 Atención de solicitudes e incidentes	<p>Considerando la información en el cuadro anterior, adicional el ticket o solicitud lleva un seguimiento a través del SDP-Service Desk desde su recepción, durante su tratamiento, confirmación del cliente de su correcta atención y documentación de las evidencias, registro en la base de conocimiento, así como la documentación de las evidencias de atención y su cierre en la herramienta SDP. Todas las actividades mencionadas también están incluidas dentro del Proceso Atención de Solicitudes e Incidentes.</p>

	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD


DOCUMENTO	DOCUMENTO REFERENCIA	Descripción breve del contenido del archivo y la justificación de su creación.
c. Presentar un plan y metodologías de atención que contemple los siguientes rubros, desde el levantamiento de información, diseño y plan de implementación:	PLAN DE TRATAMIENTO DE RIESGOS FR-10-09 ED0 Análisis y Tratamiento de Riesgos a la Seguridad de Información ME-10-01 ED1 Metodología de riesgos TIFR-10-08 ED0 Formato SoA	<p>El Proceso de Seguridad de la Información también incluye diversos formatos entre estos resalta el formato de identificación de riesgos de seguridad de la información, el cual registra los posibles riesgos de todas las áreas que pudieran presentarse y el Coordinador de Sistemas evalúa las acciones para evitar a través de los diferentes dispositivos de TI y las buenas prácticas sugeridas como parte de la implementación de las normas ISO 20000-1 e ISO 27001 evitar cualquier vulnerabilidad de forma preventiva.</p> <p>Adicional se establece una Metodología de Riesgos basada en la norma ISO 31000 Gestión de Riesgos, la cual tiene como principal objetivo analizar y evaluar los riesgos de seguridad de la información. Se evalúan escenarios, grado en que se afecta la Confidencialidad, Integridad y Disponibilidad de la información (a lo anterior se le llama Ponderación del CID), adicional se hace una Estimación del riesgo inicial, Estimación de su probabilidad de ocurrencia, Clasificación de la severidad (impacto), Clasificación de la detección (controles actuales) y con los datos anteriores se determina el NPR-Nivel de Prioridad de Riesgo para evaluar su criticidad de los riesgos, y dar un tratamiento oportuno y buscar eliminar o minimizarlo. Este proceso es aplicado a la plataforma tecnológica y es complemento de los procesos sustantivos del contrato.</p> <p>De igual manera la Metodología de Riesgos incluye el formato FR-10-08 Formato SoA que describe los 114 controles establecidos en el Anexo A de la norma ISO 27001 Gestión de Seguridad de la Información y las actividades que se realizan para dar cumplimiento a estos controles aceptados por parte de Grupo Siayec y se implementan en la Suprema Corte de Justicia de la Nación.</p>
<ul style="list-style-type: none"> Seguridad de los datos: El acceso a la información y la tecnología debe basarse en la necesidad de conocer, sobre la base de la función laboral. 	MATRIZ DE PERFILES DE USUARIO MT-10-02 ED1 Matriz de perfiles Grupo Siayec	Este formato Matriz de Perfiles, describe los puestos de los diferentes niveles de la organización y de acuerdo a cada categoría, se asigna un perfil, se estandariza 4 perfiles y se asigna un token de usuario con privilegios por cada usuario, ya dependerá del nivel el que tengan o no ciertos privilegios de acceso a los diferentes aplicativos y áreas controladas.

	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD


DOCUMENTO	DOCUMENTO REFERENCIA	Descripción breve del contenido del archivo y la justificación de su creación.
<ul style="list-style-type: none"> Procedimientos para la revisión periódica de informes u otras listas de autorización de derechos de acceso de usuarios. 	<p>PROCESO DE REVISIÓN DE MATRIZ</p> <p>Proceso PC-10-01-01 ED1 Alta Baja y Cambio de usuarios</p>	<p>A través del proceso Alta Baja y Cambio describe las actividades para realizar el alta, baja y cambio de usuarios a los diferentes aplicativos estándar de TI, para el desempeño de su actividad. Dentro del proceso se establece la MT-10-02 Matriz de perfiles la cual se describe en el cuadro anterior. Esta actividad ayuda a controlar y limitar a los diferentes dispositivos, aplicativos y áreas controladas.</p>
<ul style="list-style-type: none"> Procedimientos para administrar el acceso asociado con los empleados que son despedidos o transferidos. 	<p>PROCESO ABC DE USUARIOS</p> <p>Proceso PC-10-01-01 ED1 Alta Baja y Cambio de usuarios</p> <p>MA-10-03 ED0 Manual de integración y funcionan Comité Seg Info.</p>	<p>Al ingreso de personal nuevo, el área de RH hace requerimiento a través de formato autorizado al área de TI, para que se configure sus equipos PC o laptop y se establezcan los privilegios de acceso.</p> <p>A la salida de alguna persona de la organización, RH informa a TI revise y de la baja de los accesos otorgados previo a su retiro de la organización. Por su parte el Área de Infraestructura realiza estas actividades con base en el Proceso Alta Baja y Cambio de usuarios, mientras que el Área de Recursos Humanos, lo gestiona a través del Proceso de Recursos Humanos, con base en sus procedimientos, Alta, Baja y Procedimiento Disciplinario.</p> <p>Y en los casos en que se pudiera presentar un incidente grave, se reúne el Comité de Seguridad de la Información para establecer acuerdos y determinar si pudiera existir algún caso de despido y el tratamiento que se dará.</p>
<ul style="list-style-type: none"> Registros para identificar el uso o el intento de uso, y la modificación o el intento de modificación de los componentes críticos del sistema. 	<p>LOGS</p> <p>Ejemplo - Evidencia logs 20221112</p>	<p>Se anexa imagen como evidencia del correcto funcionamiento del monitoreo de los logs.</p>

	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 <p>Suprema Corte de Justicia de la Nación</p>
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD


DOCUMENTO	DOCUMENTO REFERENCIA	Descripción breve del contenido del archivo y la justificación de su creación.
<ul style="list-style-type: none"> Utilizar y mantener herramientas de configuración/administración de estado del sistema, se debe registrar la asignación y el uso de todas las cuentas con capacidades de acceso privilegiado. 	<p>MATRIZ DE PERFILES DE USUARIO</p> <p>MT-10-02 ED1 Matriz de perfiles Grupo Siayec</p>	<p>Los privilegios de acceso a herramientas de configuración están definidos y previamente autorizados por la Gerencia de Infraestructura TI, y documentados dentro de la Matriz de perfiles MT-10-02.</p>
<ul style="list-style-type: none"> Los registros deberán estar debidamente protegidos contra el acceso no autorizado. 	<p>PROCESO ABC DE USUARIOS</p> <p>Proceso PC-10-01-01 ED1 Alta Baja y Cambio de usuarios</p>	<p>La organización cuenta con una política de control de acceso a la información física y digital. Se establece un proceso formal y política de seguridad física. Se establecen puntos de acceso de carga y descarga en las instalaciones, los cuales se controlan para evitar un acceso no controlado. Se establecen áreas controladas para los equipos del site, de los IDF's, con el fin de mantenerlos en óptimas condiciones y bajo control contra los factores externos que pudieran afectarlos.</p>
<ul style="list-style-type: none"> Proceso documentado sobre cómo se realizan las copias de seguridad del sistema, la aplicación y los datos. Describir la rutina para las copias de seguridad (completas, incrementales, diferenciales; continuas, diarias, semanales, etc.). 	<p>PROCESO DE RESPALDOS</p> <p>Proceso PC-10-01-01-03 ED1 Respaldos</p>	<p>A través del proceso de respaldos se garantiza la protección y control de los registros importantes para la organización.</p>

	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

DOCUMENTO	DOCUMENTO REFERENCIA	Descripción breve del contenido del archivo y la justificación de su creación.
<ul style="list-style-type: none"> Todos los medios de copia de seguridad, tanto en el sitio, fuera del sitio, completos y / o incrementales, deben volverse ilegibles al final de su vida útil, y deberán estar protegidos contra el acceso no autorizado y la manipulación. 	<p>PROCESO DE BORRADO SEGURO</p> <p>Proceso PC-10-01-05 ED0 Borrado Seguro</p>	<p>Se establece en la política de seguridad de la información y en proceso formal, que la Gerencia de Infraestructura TI es la única autorizada para gestionar los medios removibles, con el fin de reducir el riesgo de fuga de información sensible que se encuentre almacenada en soportes que se desechen o reutilicen.</p>
<ul style="list-style-type: none"> Todos los medios de copia de seguridad que contengan información confidencial deben cifrarse y almacenarse de forma segura. 	<p>PROCEDIMIENTO DE RESGUARDO SEGURO Y RESTRICCIÓN</p> <p>Proceso PC-10-01-01-03 ED1 Respaldos.</p> <p>Proceso PC14 ED3 Servicios Generales (este incluye el Procedimiento de Control de Acceso).</p>	<p>Se establece proceso formal para asegurar que la información pueda ser recuperada después de un posible desastre o falla, de manera que la continuidad del proceso se mantenga.</p> <p>También se establece procedimiento formal de control de acceso a las instalaciones de la Organización.</p>
<ul style="list-style-type: none"> Verificar la identidad y los antecedentes de todo su personal en función de las verificaciones de antecedentes de seguridad. describir las actividades de detección realizadas a los proveedores y solicitantes de empleo (por ejemplo, crédito, detección de drogas, referencias y verificaciones de antecedentes penales). 	<p>PROCESO R.H. / FINANZAS / COMPRAS</p> <p>Proceso PC-11 ED11 Recursos Humanos</p> <p>Proceso PC-12 ED3 Finanzas (dentro incluye el Procedimiento de Compras).</p>	<p>La Gerencia de Recursos Humanos da instrucción para que se realicen los estudios socioeconómicos para la evaluación de antecedentes y evaluación de referencias laboral y personales.</p> <p>En lo que se refiere a los proveedores, se les solicita documentación fiscal que acredite su confiabilidad, y su revisión en la lista del SAT que no tenga ningún antecedente y se establecen los acuerdos de confidencialidad.</p>


	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

DOCUMENTO	DOCUMENTO REFERENCIA	Descripción breve del contenido del archivo y la justificación de su creación.
<ul style="list-style-type: none"> Se deberá impedir que los empleados o proveedores de servicios con acceso a la información de la Suprema Corte de Justicia de la Nación trabajen antes de completar las verificaciones de antecedentes. 	PROCESO R.H. / FINANZAS / COMPRAS Proceso PC-11 ED11 Recursos Humanos Proceso PC-12 ED3 Finanzas (dentro incluye el Procedimiento de Compras)	No existe contratación hasta que las pruebas del estudio socioeconómico son entregadas.
<ul style="list-style-type: none"> Los empleados Grupo Siayec firman un acuerdo de confidencialidad o no divulgación. 	ACUERDO DE CONFIDENCIALIDAD Carta de Confidencialidad	Es una política obligatoria permanente el hecho de que todo el personal de nuevo ingreso a la organización debe firmar "Acuerdo de confidencialidad", así como de "Protección de datos personales", lo anterior lo gestiona RH al ingreso de personal nuevo a la organización.
<ul style="list-style-type: none"> Programa de transferencia de conocimiento y entrenamiento, y concientización de seguridad para todos los empleados (personal nuevo, existente, permanente, temporal o contratado). Desarrollar el Programa y la frecuencia de la recertificación o reeducación. 	PROCESO DE GESTIÓN DEL CONOCIMIENTO Proceso PC2 ED4 Gestión del conocimiento	La organización cuenta con una plataforma interna llamada SIAYEC ACADEMIC a través de la cual se implementan capacitaciones de acuerdo de acuerdo a las actividades que realizan internamente dentro de la organización. Y la gestión del conocimiento que se genera como parte de su aprendizaje, se documenta en la base de conocimiento.

	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD



MODELO DEL SISTEMA



	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD



DECLARACIONES Y EXCLUSIONES

Durante la operación del servicio administrado para la solución de seguridad de la Suprema Corte de Justicia de la Nación, este manual servirá como medio de auditoría y cumplimiento de los alcances del contrato en su fase 3.

 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

ESTRUCTURA DOCUMENTAL



Tipo de Documento	Descripción
Política y Objetivos	<p>La política es el compromiso respecto a la calidad de gestión de los servicios que ampara el contrato de referencia, así como la seguridad de la información. Los objetivos serán la herramienta para la mejora continua del Sistema integral de gestión de Riesgos, estos deberán establecerse en tres niveles durante la prestación del servicio:</p> <p>Estratégicos: para la ejecución de los servicios</p> <p>Tácticos: para la implementación de los procesos: Operativos: para aplicar a los operadores y personas relacionadas.</p>
Manuel del Sistema de gestión	<p>Documento que especifica la estructura, la organización y la lógica del funcionamiento del Sistema de Gestión Integral de Seguridad e incluye los estándares ISO con los cuales gestiona sus procesos</p>
Procedimientos e instrucciones de trabajo	<p>Son las especificaciones para llevar a cabo los procesos. Las instrucciones de trabajo describen una actividad o grupo de actividades y están subordinados a los procedimientos</p>
Formatos y registros	<p>Son la evidencia de los procesos del Sistema de gestión, la mayoría se llevan en un formato permitiendo su estandarización y control.</p>

 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

APROBACIONES



Clave	Nombre del Documento	Edición	Fecha:
	Documento maestro del Sistema Integral de Seguridad para la Gestión del Riesgo	00	31/12/2022

Elabora	Revisa	Aprueba
Norberta Olivares Álvarez Coordinadora de calidad y procesos Grupo Siayec		

 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

CONTROL DE CAMBIOS

Edición	Fecha	Apartado o Anexo	Descripción
00	31/12/2022	Documento maestro del Sistema Integral de Seguridad para la Gestión Integral del Riesgo	Primera emisión

 GRUPO SIAYEC	"SERVICIO ADMINISTRADO PARA LA SOLUCIÓN DE SEGURIDAD DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN - ETAPA 1"	 Suprema Corte de Justicia de la Nación
	CONTRATO: SCJN/DGRM/DPC-014/07/2022	REFERENCIA: 09. DOCUMENTOS DE DISEÑO DEL SISTEMA INTEGRAL DE SEGURIDAD

DOCUMENTOS DE REFERENCIA

Anexo 1 - Matriz de riesgos

Anexo 2 - Protocolos de actuación