Firma Digital

Firmado digitalmente por ALVAREZ QUISPE Mario Alejandro FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 30.09.2024 14:41:57 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 30.09.2024 15:19:41 -05:00

Firma Digital

Firmado digitalmente por SIFUENTES DEL MAR Rafael Nicolas FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 30.09.2024 16:13:46 -05:00

Junta Nacional de Justicia

RESOLUCIÓN Nº 089-2024-DG-JNJ

San Isidro, 30 de setiembre de 2024

VISTOS:

El memorando N° 000644-2024-OTIDG/JNJ de la Oficina de Tecnologías de la Información y Gobierno Digital, y el Informe N° 00212-2024-OPCT/JNJ de la Oficina de Planificación y Cooperación Técnica; y,

CONSIDERANDO:

La Ley de Gobierno Digital, aprobada por el Decreto Legislativo N° 1412, establece un marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

El Reglamento de la Ley de Gobierno Digital, aprobado por Decreto Supremo N° 029-2021-PCM, señala en el numeral 109.1 del artículo 109, que el Sistema de Gestión de Seguridad de la Información (SGSI), comprende el conjunto de políticas, lineamientos, procedimientos, recursos y actividades asociadas, que gestiona una entidad con el propósito de proteger sus activos de información, de manera independiente del soporte en que estos se encuentren. Asimismo, contempla la gestión de riesgos e incidentes de seguridad de la información y seguridad digital, la implementación efectiva de medidas de ciberseguridad, y acciones de colaboración y cooperación;

El numeral 109.3 del artículo 109 del referido Reglamento dispone que las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), teniendo como alcance mínimo sus procesos misionales y aquellos que son relevantes para su operación;

Mediante Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, se dispone que el Plan de implementación del Sistema de Gestión de Seguridad de la Información es el instrumento que establece, como mínimo, los objetivos, actividades, recursos, responsables y plazos para implementar un Sistema de Gestión de Seguridad de la Información, en un periodo máximo de tres (03) años. Es aprobado por la máxima autoridad administrativa o la que haga sus veces en la entidad pública;

Firma Digital

Firmado digitalmente por ALVAREZ QUISPE Mario Alejandro FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 30.09.2024 14:42:05 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 30.09.2024 15:20:17 -05:00

Firma Digital

Firmado digitalmente por SIFUENTES DEL MAR Rafael Nicolas FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 30.09.2024 16:14:10 -05:00

Junta Nacional de Justicia

Al respecto, la Oficina de Tecnologías de la Información y Gobierno Digital propone el Plan de Implementación del Sistema de Gestión de Seguridad de la Información de la Junta Nacional de Justicia 2025 - 2027; plan que ha sido revisado por la Oficina de Planificación y Cooperación Técnica;

De acuerdo con el artículo 16 del Reglamento de Organización y Funciones la Dirección General se constituye en la máxima autoridad administrativa de la Junta Nacional de Justicia, por lo que corresponde emitir el acto administrativo por el que se apruebe el referido plan;

De conformidad con lo dispuesto en Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD y en el Reglamento de Organización y Funciones de la Junta Nacional de Justicia; y, con el visado de los jefes de las Oficinas de Tecnología de la Información y Gobierno Digital, de Planificación y Cooperación Técnica y de Asesoría Jurídica;

SE RESUELVE:

Artículo 1. Aprobar el Plan de Implementación del Sistema de Gestión de Seguridad de la Información de la Junta Nacional de Justicia 2025 – 2027 y su anexo 01, los que forman integrante de la presente resolución.

Artículo 2. Disponer que la Oficina de Tecnologías de la Información y Gobierno Digital efectúe las acciones que correspondan para la implementación de las actividades programadas en el Plan aprobado en el artículo 1 de la presente resolución.

Artículo 3. Disponer la publicación de la presente resolución y su anexo, en el portal de transparencia y en el portal institucional de la Junta Nacional de Justicia (www.gob.pe/jnj).

Regístrese, comuníquese y publíquese.

Firma Digital

Firmado digitalmente por MARRUJO ASTETE Betty Liliana FAU 20194484365 soft
Motivo: Soy el autor del documento
Fecha: 30.09.2024 19:56:43 -05:00

BETTY LILIANA MARRUJO ASTETE
DIRECTORA GENERAL
JUNTA NACIONAL DE JUSTICIA

Junta Nacional
de Justicia

PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA JUNTA NACIONAL DE JUSTICIA

2025-2027

Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:45:52 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:02:52 -05:00

INDICE

Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:46:00 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:03:08 -05:00

I. INTRODUCCIÓN

El Estado Peruano, a través de la Política General de Gobierno aprobada por Decreto Supremo N° 042-2023-PCM establece entre otras disposiciones que, las entidades públicas hacen uso intensivo de las tecnologías digitales y datos para el cumplimiento de la Política General de Gobierno, en el marco del proceso nacional de transformación digital.

Asimismo, de acuerdo a lo establecido en el Artículo 3° del Decreto Legislativo N° 1412, Ley de Gobierno Digital (en adelante, la Ley de Gobierno Digital), el gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público.

En este contexto, la Presidencia del Consejo de Ministros a través de la Secretaría de Gobierno y Transformación Digital, viene impulsando el proceso de transformación digital en las entidades de la administración pública coadyuvando a la generación de valor público de cara al ciudadano mediante la prestación de servicios digitales que garanticen la disponibilidad, integridad y confidencialidad de la información.

De igual manera, el Reglamento de la Ley de Gobierno Digital aprobado mediante Decreto Supremo N°029-2021-PCM en su Artículo 105° establece que las entidades públicas tienen entre sus obligaciones implementar y mantener un Sistema de Gestión de Seguridad de la Información (en adelante, el SGSI). Asimismo, en su Artículo 109° se precisan algunas disposiciones para la definición del alcance, diseño, implementación, operación y mejora del SGSI.

Así también, con Resolución de Secretaría de Gobierno y Transformación Digital N° 0032023-PCM/SGTD, de fecha 06 de setiembre de 2023, se establece la Implementación y Mantenimiento del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas, así mismo, en su artículo 1 se indica que las entidades públicas deben utilizar obligatoriamente la Norma Técnica Peruana NTP ISO/IEC 27001 vigente para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.

El Plan de implementación del Sistema de Gestión de Seguridad de la Información en la Junta Nacional de Justicia (Plan SGSI), establece el marco de implementación del SGSI bajo el estándar NTP ISO/IEC 27001:2022, contemplando los objetivos, alcance, los recursos, cronograma de actividades, mecanismos de monitoreo, entre otros, a desarrollarse durante el periodo 2025-2027

II. OBJETIVOS DEL PLAN DEL SGSI

Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la NTP ISO/IEC 27001:2022, en cumplimiento de los objetivos de seguridad de la información, de acuerdo a las recomendaciones establecidas en los estándares y norma técnica peruana para la Gestión de la Seguridad de la Información.

Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:46:07 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:03:19 -05:00

III. MARCO LEGAL

3.1. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado
3.2. Ley Nº 29733, Ley de Protección de Datos Personales y su reglamento, aprobado mediante Decreto Supremo Nº 003-2013.JUS.
3.3. Decreto Legislativo N°1412, Ley de Gobierno Digital
3.4. Decreto de Urgencia N° 006-2020 que crea el Sistema Nacional De Transformación Digital.
3.5. Decreto de Urgencia N° 007-2020 que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
3.6. Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece las tecnologías y medios electrónicos en el procedimiento administrativo.
3.7. Decreto Supremo N° 103-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.
3.8. Decreto Supremo N° 085-2023-PCM, Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030.
3.9. Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Seguridad de la Información en las Entidades Públicas y en el artículo 3 indica el desarrollo del plan de implementación del SGSI.
3.10. Resolución N° 190-2020-JNJ del 24 de setiembre de 2020 que conforma el comité de gobierno digital en la Junta Nacional de Justicia.
3.11. Resolución N° 816-2024-JNJ que modifica la conformación del comité de gobierno digital en la Junta Nacional de Justicia.

IV. TÉRMINOS Y DEFINICIONES

4.1. Activo de Información: Cualquier elemento físico, tecnológico o intangible que genera, almacena o procesa Información y tiene valor para la organización, como base de datos, archivos, programas, manuales, equipos de comunicaciones, la imagen de la entidad, la Información como activo corporativo, puede existir de muchas formas (impresa, almacenada electrónicamente, transmitida por medios electrónicos, mostrada en videos, suministrada en una conversación, conocimiento de las personas).
4.2. Amenazas: Fuentes generadoras de eventos en las que se originan las pérdidas por riesgos de seguridad de la información.
4.3. Análisis de riesgo: Método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.
4.4. Auditoria: Proceso sistemático, independiente y documentado para obtener evidencias que, al evaluarse de manera objetiva, permite determinar la extensión en que se cumplen los criterios definidos para la auditoría interna.
4.5. Control: Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de la organización.
4.6. Declaración de Aplicabilidad: Documento que describe los objetivos de control y los controles pertinentes y aplicables para el sistema de gestión de seguridad

Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:46:14 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:03:30 -05:00

de la información de la entidad.

4.7. Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para el uso; la no disponibilidad de la información puede resultar en pérdidas financieras de imagen y/o credibilidad ante los clientes y/o ciudadanos.
4.8. Efectividad: Medida de impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.
4.9. Eficacia: Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.
4.10. Estimación de riesgo: Proceso de asignación de valores a la probabilidad e impacto de un riesgo.
4.11. Evento de seguridad de la información: Presencia identificada de una condición de un bien o recurso (sistema, servicio, red, etc), asociada a una posible vulneración de la política de seguridad de la información.
4.12. Evidencia de auditoria: Registro, declaración de hechos o cualquier otra información que son relevantes para los criterios de auditoría y que son verificables. La evidencia de la auditoria puede ser cuantitativa o cualitativa.
4.13. Gestión de riesgo: Actividades coordinadas para dirigir y controlar los aspectos asociados al riesgo dentro de una organización.
4.14. Identificación del riesgo: Proceso para encontrar, numerar y caracterizar los elementos de riesgo asociadas a la seguridad de la información.
4.15. Impacto: Se establece como la consecuencia directa o indirecta de la materialización de los escenarios de riesgo generando cambios adversos en los objetivos de la organización.
4.16. Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tiene una probabilidad significativa de comprometer las operaciones de la organización y amenazar la seguridad de la información.
4.17. Información: Datos relacionados que tienen significado para la organización. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada.
4.18. Integridad: La información de la entidad debe ser clara y completa y solo podrá ser modificada por las personas expresamente autorizadas para ello.
4.19. Probabilidad: Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
4.20. Proceso: Conjunto de actividades relacionadas mutuamente o que interactúan para generar valor y cuales transforman elementos de entrada en resultados.
4.21. Propietario de información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones de acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. El término “Propietario” no implica que la persona tenga realmente los derechos de propiedad de los activos.
4.22. Reducción de riesgo: Acciones que se toman para disminuir la probabilidad y/o el impacto negativo asociado a un riesgo.
4.23. Responsabilidades: Compromisos u obligaciones del personal o grupo de trabajo.
4.24. Riesgo: Consecuencias que pueden ser generadas por las amenazas asociadas a la seguridad de la Información en los activos.

Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:46:23 -05:00

Firma Digital

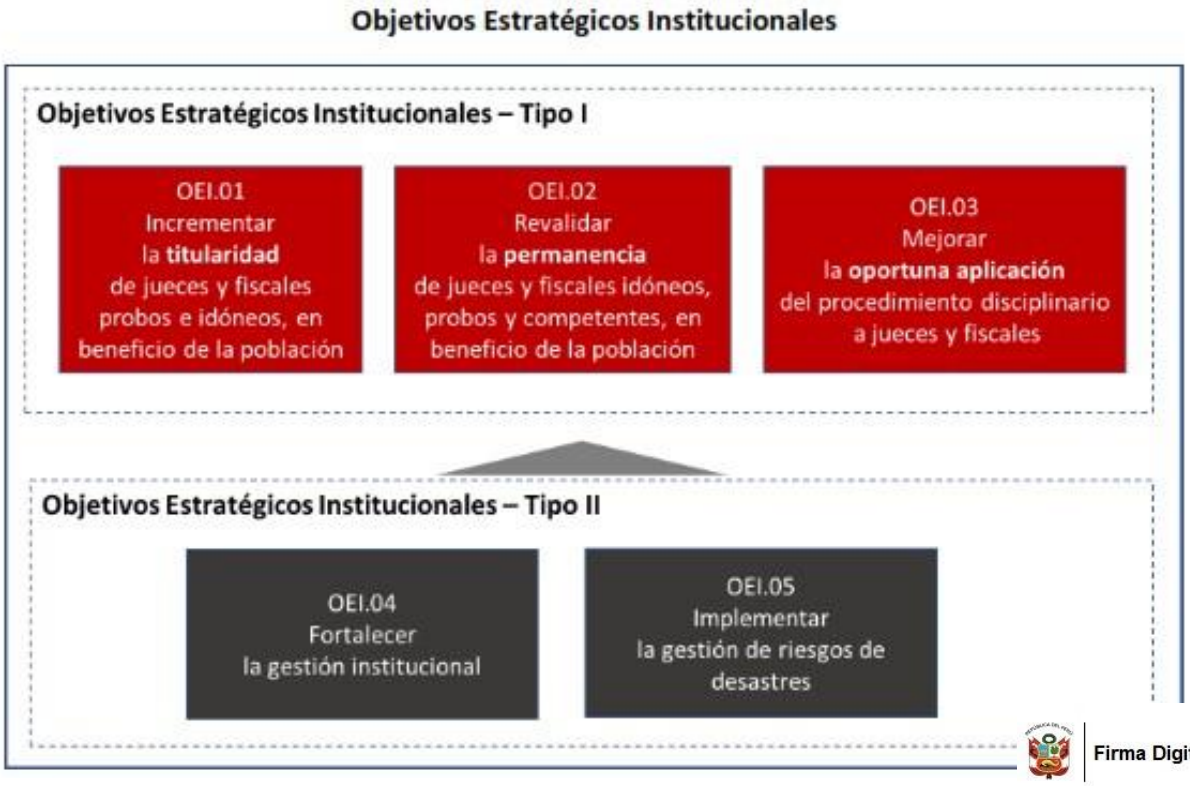
Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:03:40 -05:00

4.25. Seguridad de la Información: Preservación de la integridad, la confidencialidad, y la disponibilidad de la Información; además puede involucrar otras propiedades tales como autenticidad, trazabilidad, no repudio y fiabilidad.
4.26. SGSI: Sistema de Gestión de Seguridad de la Información.
4.27. Transferencia de riesgo: Compartir con otra de las partes la perdida (consecuencias negativas) de un riesgo.
4.28. Tratamiento de la Información: Desarrollo de las siguientes actividades sobre la Información, sin limitarse a ellas: creación, acceso, inclusión, exclusión, corrección, comunicación, divulgación, publicación, cesión, eliminación y certificación; por cualquier medio oral, digital y/o escrito, conocido o por conocer.
4.29. Tratamiento del riesgo: Proceso de selección e implementación de medidas para modificar el riesgo.
4.30. Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice Información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de Información, para propósitos propios de su labor y que tendrá el derecho manifiesto de uso dentro del inventario de Información.
4.31. Vulnerabilidades: Debilidad de un activo de Información frente a una amenaza.
4.32. Conformidad: Cumplimiento de un requisito.

V. CONTEXTO DE LA ENTIDAD

5.1. ALINEACIÓN A LOS OBJETIVOS ESTRATEGICOS DE LA JNJ

El Plan Estratégico Institucional (PEI) 2021-2027, aprobado mediante Resolución de la Dirección General N°024-2024-DG-JNJ, considera como objetivos estratégicos institucionales lo siguiente:



Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:46:35 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:03:50 -05:00

Para alcanzar los objetivos estratégicos Tipo 1 y Tipo 2 es necesario contar con sistemas y procesos administrativos y misionales óptimos, y se debe reforzar la seguridad de la información en ellos a fin de garantizar la confidencialidad, integridad y disponibilidad, es por ello que la Junta Nacional de Justicia en cumplimiento del Decreto Supremo N°029-2021-PCM implementará el Sistema de Gestión de Seguridad de la Información de la JNJ bajo la NTP ISO/IEC 27001:2022, estándar internacional que establece los requisitos para la gestión de la seguridad de la información en un organización; asimismo para la implementación de los controles de seguridad se tomara en cuenta la norma NTP ISO/IEC 27002:2022.

5.2. SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LA JNJ

La Junta Nacional de Justicia viene realizando acciones a fin de cumplir con la normativa en seguridad de la información.

Mediante Resolución N°019-2023-DG/JNJ se aprobaron los Lineamientos Técnicos para la seguridad de la Información en la Junta Nacional de Justicia, cuyo objetivo es establecer mecanismos para la protección de la confidencialidad, integridad y disponibilidad de la información en los diferentes procesos que se realizan en la entidad.

Asimismo, se conformó el Comité de Gobierno y Transformación Digital, asimismo, mediante Resolución N°064-2023-P-JNJ se designa al Oficial de Seguridad y Confianza Digital de la JNJ.

Actualmente, la entidad no cuenta con un SGSI implementado y aprobado, siendo que se desarrollará tomando en cuenta la NTP ISO/IEC 27001:2022 que es la actualmente vigente tal como lo requiere la Resolución de Secretaría de Gobierno y Transformación Digital N°003-2023-PCM/SGTD.

VI. MAPA DE PROCESOS DE LA ENTIDAD

La JNJ mediante Resolución de Presidencia N°054-2022-P-JNJ del 12 de diciembre del 2022 aprobó la versión 2.0 del mapa de procesos de la entidad la misma que consta de:

- 04 procesos estratégicos
- 05 procesos operativos
- 06 procesos de soporte

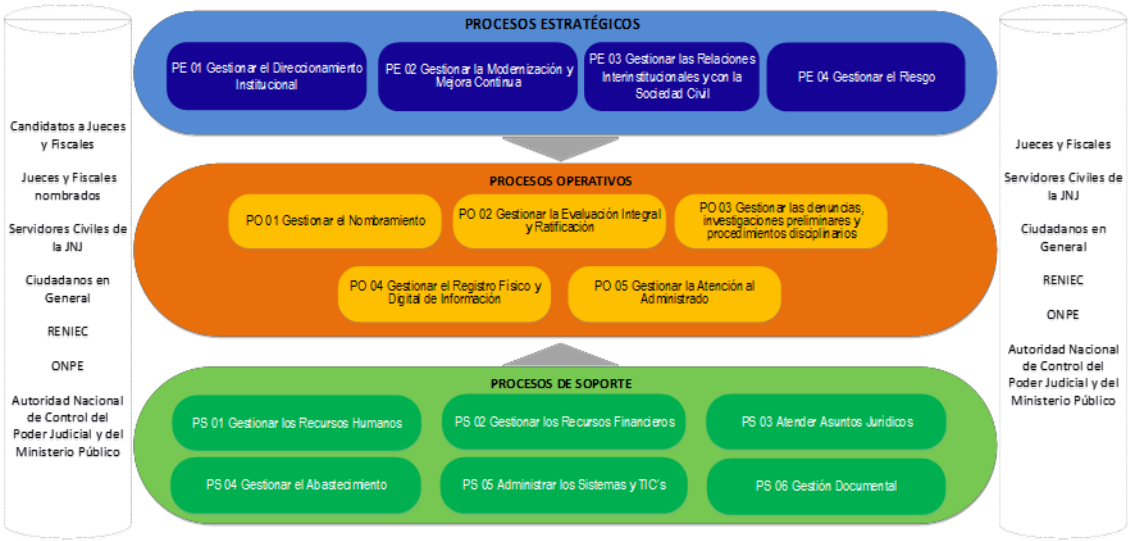
Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:46:45 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:04:01 -05:00

MAPA DE PROCESOS DE LA JNJ – NIVEL 0



VII. ALCANCE DEL SGSI:

El alcance inicial del SGSI abarcará los 3 procesos operativos, los mismos que corresponden a los procesos misionales de la entidad, y al ser los más relevantes requieren contar con el debido soporte de la seguridad de la información.

- PO01 Gestionar el Nombramiento
- PO02 Gestionar la Ratificación
- PO03 Gestionar las denuncias, investigaciones preliminares y procedimientos disciplinarios.

Asimismo, considerará el proceso de soporte PS05 Administrar los sistemas y TIC´s, que es indispensable para el adecuado funcionamiento de los procesos operativos.

Cada proceso en donde se implementará el SGSI se realizará de acuerdo al ciclo de vida de mejora continua PHVA (Planificar, hacer, verificar y actuar).

VIII. CRONOGRAMA DE ACTIVIDADES

La implementación del SGSI en la Junta Nacional de Justicia se realizará de acuerdo al cronograma indicado en el anexo 1.

IX. RECURSOS Y PRESUPUESTO:

a) <u>Personal:</u>

El desarrollo de las actividades del Plan de Implementación del SGSI abarca los siguientes recursos de acuerdo a lo señalado en la Artículo 5 de la RESOLUCIÓN DE SECRETARÍA DE GOBIERNO Y TRANSFORMACIÓN DIGITAL N° 003-2023-PCM/SGTD.

- Equipo de trabajo técnico y multidisciplinario encargado de realizar la

Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:46:55 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:04:11 -05:00

implementación y mantenimiento del SGSI en la entidad, dicho equipo de trabajo es liderado por el Oficial de Seguridad y Confianza Digital.

La máxima autoridad administrativa deberá designar el equipo de trabajo multidisciplinario una vez de aprobado el presente Plan de Implementación.

b) Presupuesto:

El presupuesto contempla el personal dedicado para el desarrollo y seguimiento del Plan del SGSI, así como las contrataciones de servicios necesarias para garantizar la implementación y mantenimiento de controles del SGSI.

El presupuesto para la contratación de servicios será cargado a la Actividad Operativa AO 05 Gestión de la seguridad y confianza digital de la Oficina de Tecnologías de la Información Digital; asimismo de requerirse recursos adicionales como el caso de auditorías, adquisición de equipos o consultorías se realizará la coordinación con la Dirección General y la Oficina de Presupuesto para la asignación de recursos.

El presupuesto estimado es de S/.70,000.00 soles, la misma que incluye el análisis de brechas inicial, la auditoría externa y la contratación del proceso de certificación en la ISO 27001:2022 de un subproceso misional de la Dirección de Selección y Nombramiento.

Año	Presupuesto	Servicio	Mes a contratar
2025	S/. 20,000.00	Análisis de brechas	Mayo
2026	S/. 25,000.00	Auditoría externa	Noviembre
2027	S/. 25,000.00	Certificación ISO 27001:2002	Febrero

Asimismo, de ser necesario la aplicación de controles que implique la adquisición de equipamiento o software, se efectuaran las acciones necesarias para que la entidad compre lo requerido.

Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:47:07 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:04:22 -05:00

X. PRESUPUESTO

Concepto	2025				2026				2027			
	Enero-Marzo	Abril-Junio	Julio-Setiembre	Octubre-Diciembre	Enero-Marzo	Abril-Junio	Julio-Setiembre	Octubre-Diciembre	Enero-Marzo	Abril-Junio	Julio-Setiembre	Octubre-Diciembre
Conformación de equipo de implementación del SGSI		X										
Contratación del servicio de analisis de brechas Elaborar documento politica de seguridad de la información de la JNJ		20,000.00										
Inicio de implementación del SGSI FASE 0: Organización de implemetación: presentar plan de trabajo, reuniones preliminares entre miembros del equipo, agenda de entrevistas, canales de comunicación y responsables:			X									
FASE 1: Planificar: Definir alcance del SGSI, definir politica de seguridad, identificación de activos de información, matriz de riesgos, plan de tratamiento de riesgos, analisis y evaluación de riesgos identificados, estrategia de respuesta ante riesgos				X	X							
FASE 2: Hacer: Definir roles y responsabilidades del SGSI, desarrollo de documentación de seguridad (procedimientos, planes, manuales, etc), describir procesos y controles de seguridad, documentar controles, plan de capacitación					X	X						
FASE 3: Verificar: Realizar una auditoria interna al SGSI implementado, plan de acción de levantamiento de no conformidades, recomendaciones de informes, evaluar nivel de cumplimiento del SGSI post implementación							X	X				
Contratar servicio de auditoria externa del sistema de gestión de seguridad de la información de la JNJ								25,000.00				
Contratar Servicio de Certificación de sub proceso de la Dirección de Selección y Nombramiento									25,000.00			

Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:47:28 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:04:43 -05:00

XI. MONITOREO Y EVALUACIÓN

A continuación, se detallan las acciones que se realizarán para el seguimiento, monitoreo y evaluación del cumplimiento de los objetivos del Plan SGSI:

- El Oficial de Seguridad y Confianza Digital realizará el seguimiento de las actividades planificadas en el cronograma de actividades, e informará de manera trimestral a la Dirección General el avance, logros, gestión de recursos y/o dificultades en la implementación u operación del SGSI.

- La Dirección General informará semestralmente a la Presidencia de la JNJ el estado del Plan SGSI, así como las dificultades en la implementación u operación del SGSI.

Firma Digital

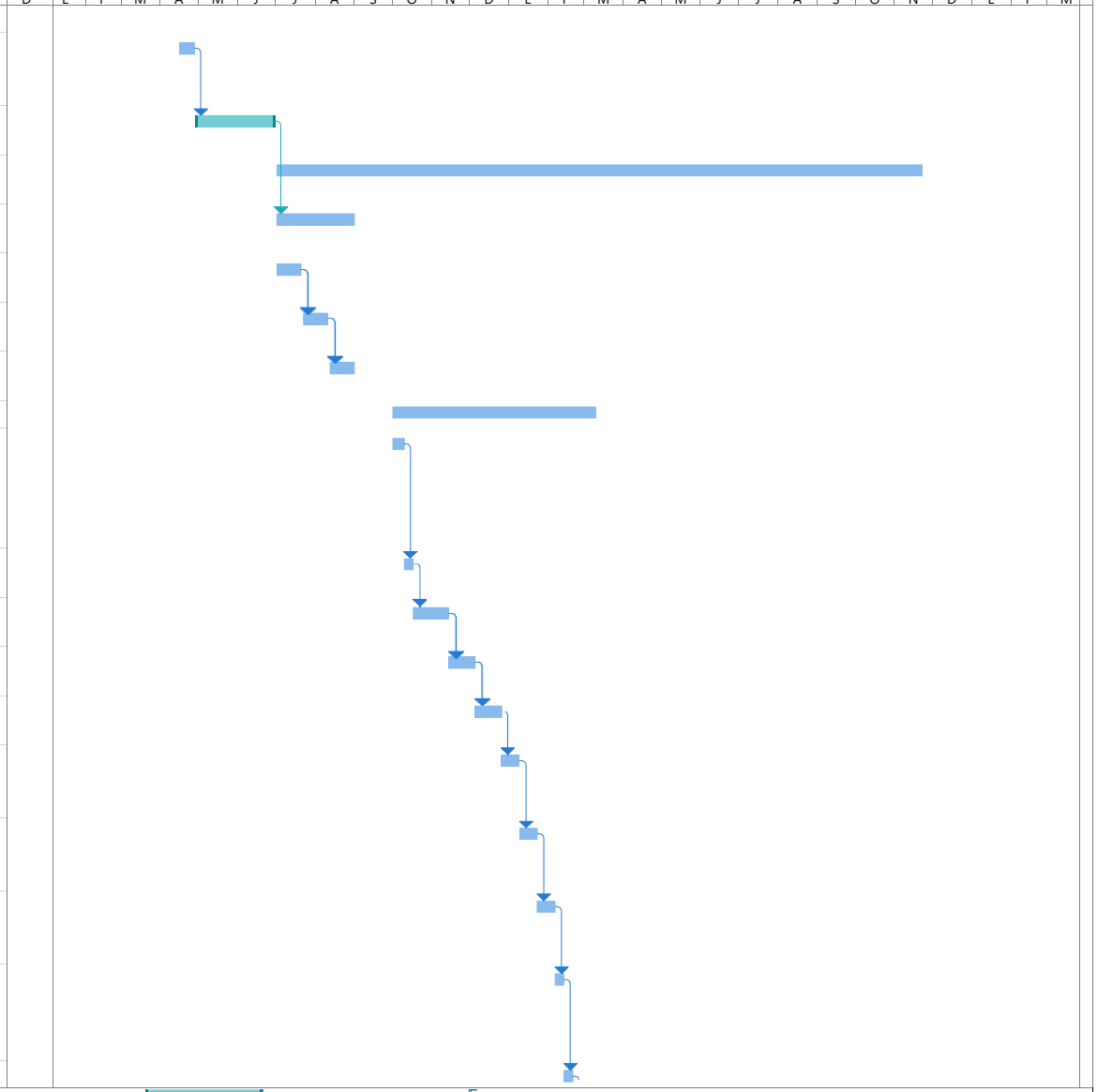
Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:47:38 -05:00

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:04:51 -05:00

ANEXO 1

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1						
2		Conformación del equipo de implementación del SGSI en la JNJ	10 días	lun 14/04/25	vie 25/04/25	
3		Contratación de consultoria de analisis de brechas del SGSI	45 días	lun 28/04/25	vie 27/06/25	2
4		Inicio de implementación del SGSI	365 días	lun 30/06/25	vie 20/11/26	
5		Fase 0 - Organización del servicio de consultoria	45 días	lun 30/06/25	vie 29/08/25	3
6		Formular Plan de trabajo de la implementación	15 días	lun 30/06/25	vie 18/07/25	
7		Realizar reuniones previas a la entrega del plan de trabajo	15 días	lun 21/07/25	vie 8/08/25	6
8		Elaborar agenda consensuada de entrevistas preliminares	15 días	lun 11/08/25	vie 29/08/25	7
9		FASE 1 - PLANIFICAR	114 días	mié 1/10/25	lun 9/03/26	
10		Definir alcance del SGSI que debe incluir los procesos misionales de DER; DSN y DPD, asi como proceso de soporte de la OTIGD	7 días	mié 1/10/25	jue 9/10/25	
11		Definir politica de seguridad de la información de la JNJ	5 días	vie 10/10/25	jue 16/10/25	10
12		Identificar los activos de información	20 días	vie 17/10/25	jue 13/11/25	11
13		Identificar riesgos positivos y negativos asociados a los activos	15 días	vie 14/11/25	jue 4/12/25	12
14		Identificar las vulnerabilidades y amenazas	15 días	vie 5/12/25	jue 25/12/25	13
15		Determinar el impacto en confidencialidad, integridad y disponibilidad de la información	10 días	vie 26/12/25	jue 8/01/26	14
16		Evaluar el impacto de los riesgos en el negocio; y objetivos institucionales.	10 días	vie 9/01/26	jue 22/01/26	15
17		Determinar la probabilidad de ocurrencia de los riesgos identificados	10 días	vie 23/01/26	jue 5/02/26	16
18		Desarrollar una matriz de probabilidad e impacto para la clasificación y priorización de los riesgos	5 días	vie 6/02/26	jue 12/02/26	17
19		Priorizar y clasificar los riesgos	5 días	vie 13/02/26	jue 19/02/26	18



Proyecto: Cronograma de imple
Fecha: mié 25/09/24

Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual

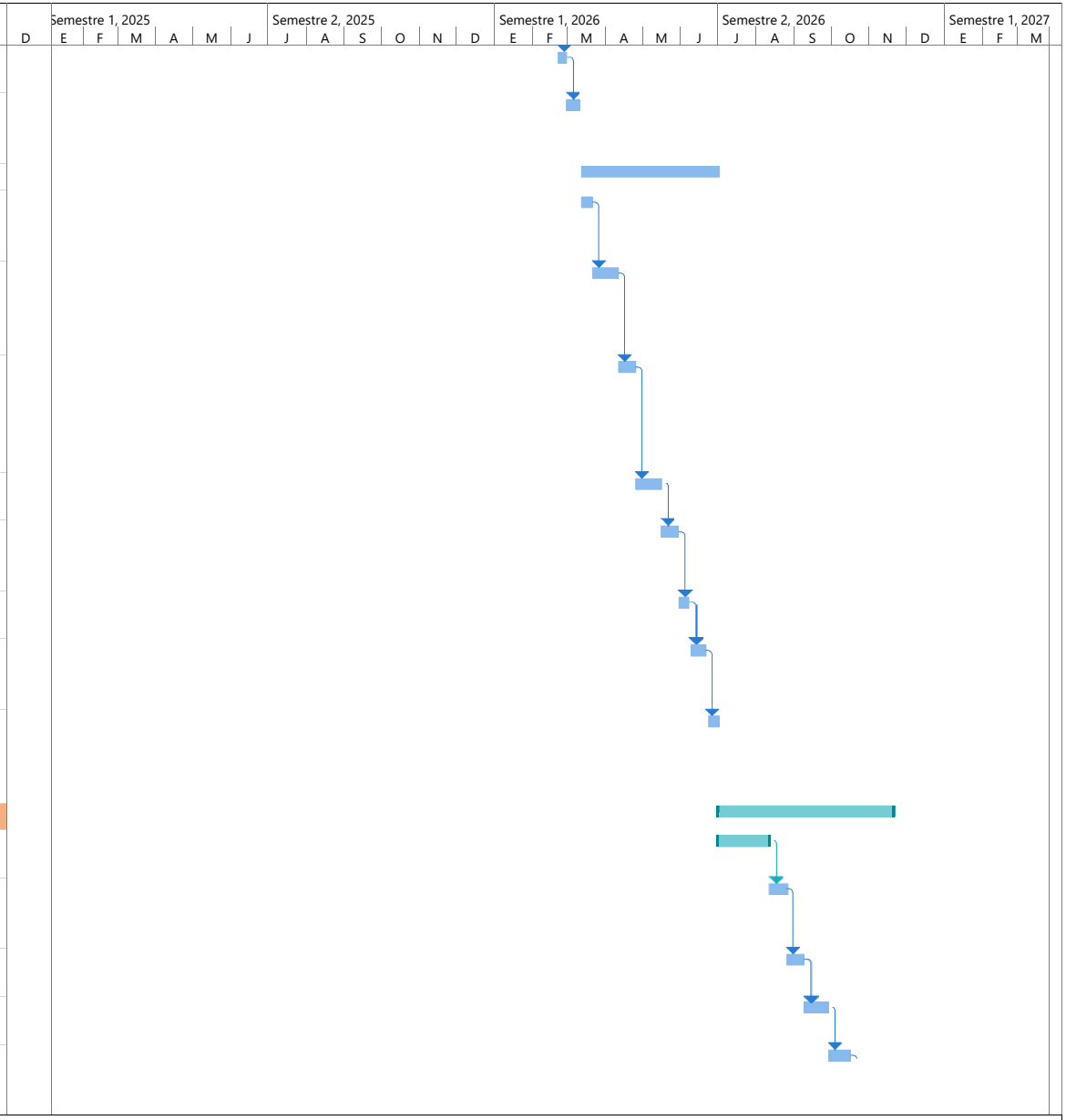
Firma Digital

Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:47:49 -05:00

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:05:24 -05:00

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
20		Definir estrategia de respuesta ante riesgos	5 días	vie 20/02/26	jue 26/02/26	19
21		Elaboración de declaración de aplicabilidad de los controles a implementar	7 días	vie 27/02/26	lun 9/03/26	20
22		FASE 2: HACER	80 días	mié 11/03/26	mar 30/06/26	
23		Definir estructura organizativa para la gestión de la seguridad de la información	7 días	mié 11/03/26	jue 19/03/26	
24		elaborar documentación requerida para el funcionamiento y mejora del SGSI	15 días	vie 20/03/26	jue 9/04/26	23
25		Elaborar procedimientos y mecanismos para realizar acciones correctivas y preventivas en el tratamiento de no conformidades	10 días	vie 10/04/26	jue 23/04/26	24
26		Documentar controles de seguridad	15 días	vie 24/04/26	jue 14/05/26	25
27		Elaborar plan de revisión periodica de la politica y alcance del SGSI	10 días	vie 15/05/26	jue 28/05/26	26
28		Desarrollar plan de capacitación en el SGSI para personal de la JNJ	6 días	vie 29/05/26	vie 5/06/26	27
29		Desarrollar taller de capacitación en el SGSI para todo el personal de la JNJ	10 días	lun 8/06/26	vie 19/06/26	28
30		Realizar gestión de incidentes y operaciones del SGSI, elaboración de politica de gestion de incidentes de la JNJ	7 días	lun 22/06/26	mar 30/06/26	29
31		FASE 3: VERIFICAR	103 días	mié 1/07/26	vie 20/11/26	
32		Realizar una auditoria interna al SGSI implementado	30 días	mié 1/07/26	mar 11/08/26	
33		Formular plan de acción para levantamiento de no conformidades	10 días	mié 12/08/26	mar 25/08/26	32
34		Remitir recomendaciones para mejora del SGSI	10 días	mié 26/08/26	mar 8/09/26	33
35		Evaluar nivel de cumplimiento del SGSI post implementación	14 días	mié 9/09/26	lun 28/09/26	34
36		Coordinar revisión de alta dirección para aprobación del SGSI	14 días	mar 29/09/26	vie 16/10/26	35



Proyecto: Cronograma de imple
Fecha: mi

Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual

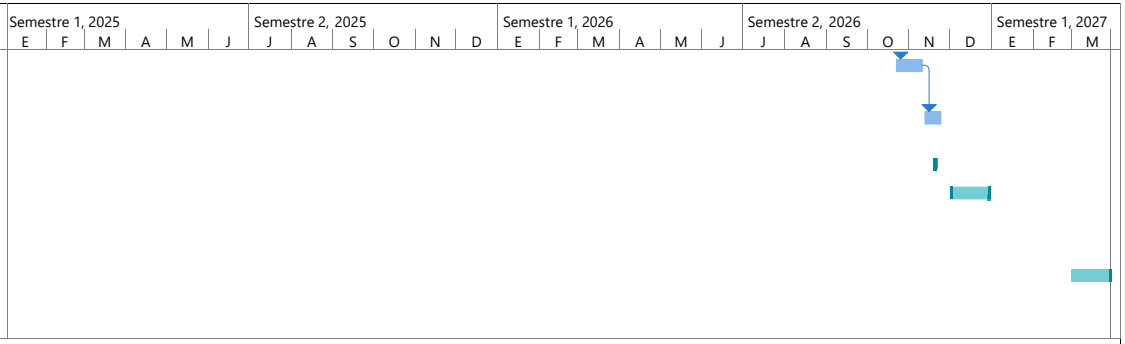
Firma Digital

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:05:36 -05:00

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:47:57 -05:00

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
37		Efectuar mejoras al SGSI en coordinación con alta dirección	15 días	lun 19/10/26	vie 6/11/26	36
38		Elaborar documentación para auditores internos de la entidad	10 días	lun 9/11/26	vie 20/11/26	37
39		FIN de implementación SGSI	1 día	vie 20/11/26	vie 20/11/26	
40		Contratar servicio de auditoria externa para revisión del SGSI de la JNJ	20 días	mar 1/12/26	lun 28/12/26	
41		Contratar servicio de certificación de subproceso de la DSN	20 días	lun 1/03/27	vie 26/03/27	



Firma Digital

Firmado digitalmente por CARPIO ANGOSTO Oscar Enrique FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 18:48:05 -05:00

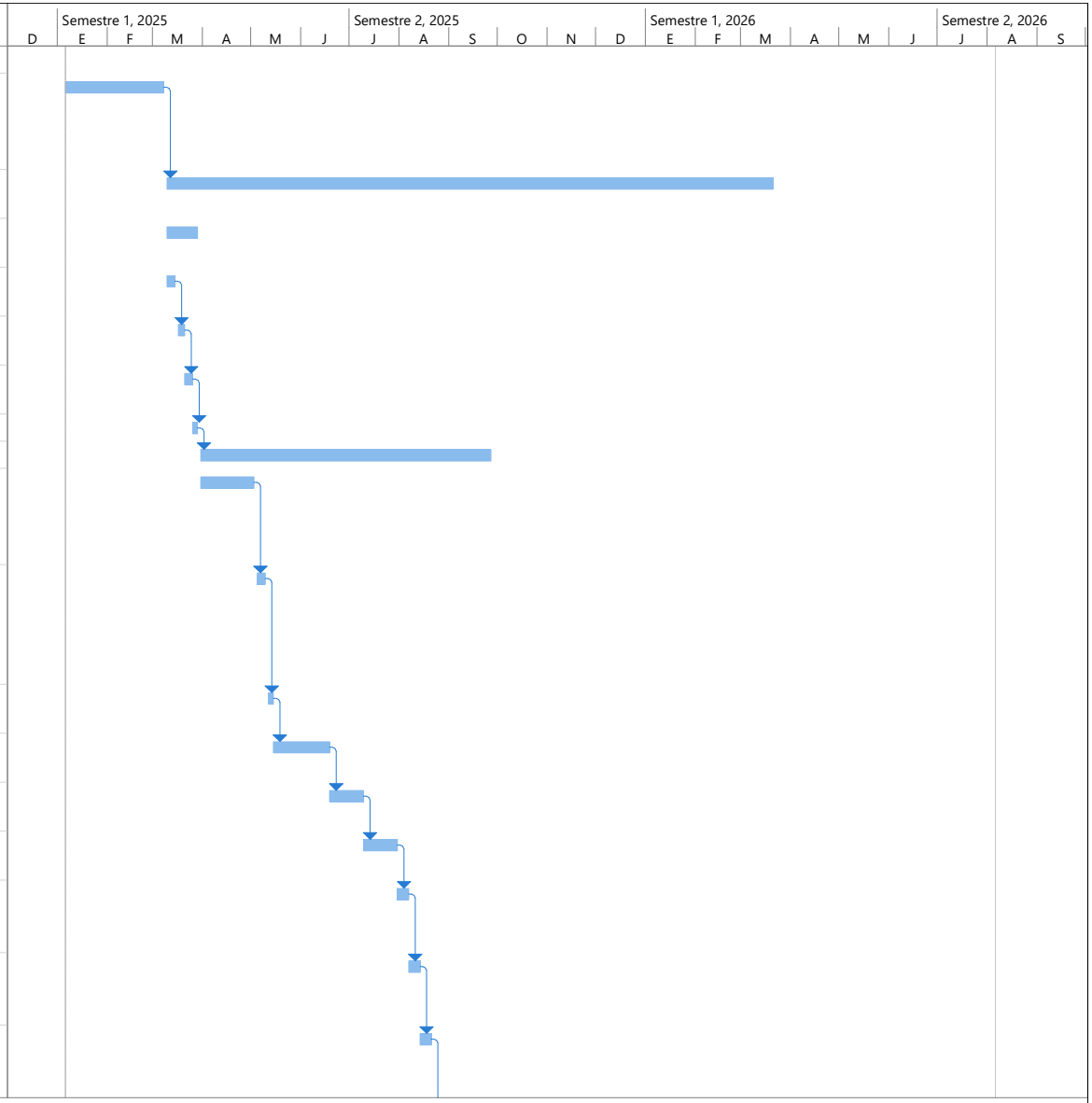
Proyecto: Cronograma de imple
Fe

Tarea | Resumen del proyecto | Tarea manual | solo el comienzo | Fecha límite
División | Tarea inactiva | solo duración | solo fin | Progreso
Hito | Hito inactivo | Informe de resumen manual | Tareas externas | Progreso manual
Resumen | Resumen inactivo | Resumen manual | Hito externo

Firma Digital

Firmado digitalmente por ALARCON BUTRON Jose Antonio FAU 20194484365 soft
Motivo: Doy V° B°
Fecha: 27.09.2024 17:05:52 -05:00

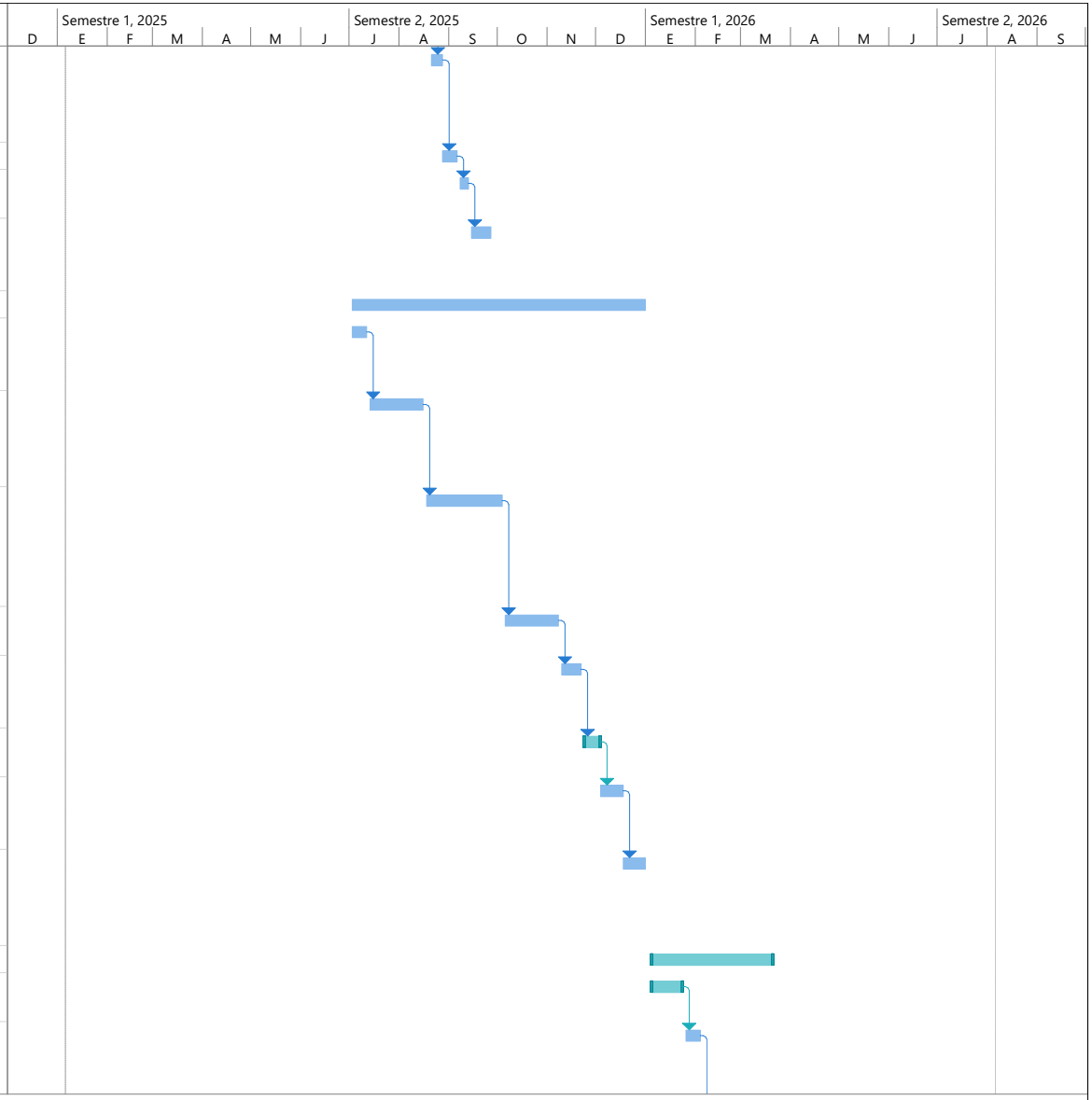
Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1						
2		Solicitud y proceso de contratación de consultoria para implementación del SGSI en la Junta Nacional de Justicia	45 días	lun 6/01/25	vie 7/03/25	
3		Inicio de consultoría para implementar SGSI	270 días	lun 10/03/25	vie 20/03/26	2
4		Fase 0 - Organización del servicio de consultoria	15 días	lun 10/03/25	vie 28/03/25	
5		Formular Plan de trabajo de la consultoria	5 días	lun 10/03/25	vie 14/03/25	
6		Realizar reuniones previas a la entrega del plan de trabajo	4 días	lun 17/03/25	jue 20/03/25	5
7		Elaborar agenda consensuada de entrevistas preliminares	3 días	vie 21/03/25	mar 25/03/25	6
8		Reunión de inicio de proyecto	3 días	mié 26/03/25	vie 28/03/25	7
9		FASE 1 - PLANIFICAR	130 días	lun 31/03/25	vie 26/09/25	8
10		Analisis de brechas: determinar la situación actual de la entidad para identificar cumplimiento de la NTP 27001	25 días	lun 31/03/25	vie 2/05/25	
11		Definir alcance del SGSI que debe incluir los procesos misionales de DER; DSN y DPD, asi como proceso de soporte de la OTIGD	5 días	lun 5/05/25	vie 9/05/25	10
12		Definir politica de seguridad de la información de la JNJ	3 días	lun 12/05/25	mié 14/05/25	11
13		Identificar los activos de información	25 días	jue 15/05/25	mié 18/06/25	12
14		Identificar riesgos positivos y negativos asociados a los activos	15 días	jue 19/06/25	mié 9/07/25	13
15		Identificar las vulnerabilidades y amenazas	15 días	jue 10/07/25	mié 30/07/25	14
16		Determinar el impacto en confidencialidad, integridad y disponibilidad de la información	5 días	jue 31/07/25	mié 6/08/25	15
17		Evaluar el impacto de los riesgos en el negocio; y objetivos institucionales.	5 días	jue 7/08/25	mié 13/08/25	16
18		Determinar la probabilidad de ocurrencia de los riesgos identificados	5 días	jue 14/08/25	mié 20/08/25	17



Proyecto: Cronograma de imple
Fecha: mar 27/08/24

Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual

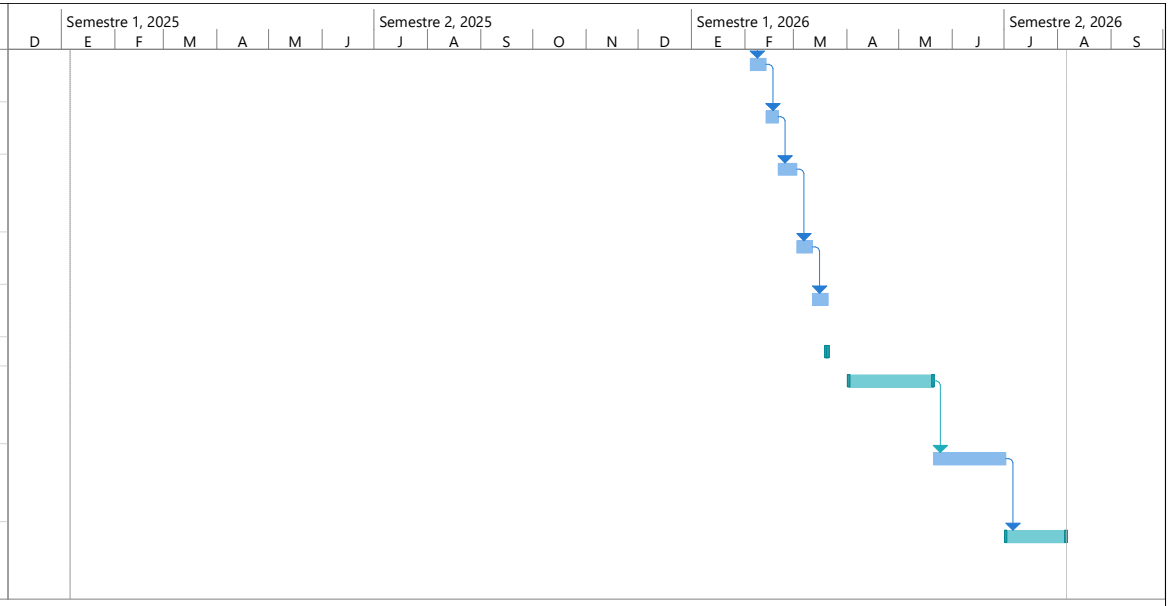
Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
19		Desarrollar una matriz de probabilidad e impacto para la clasificación y priorización de los riesgos	5 días	jue 21/08/25	mié 27/08/25	18
20		Priorizar y clasificar los riesgos	7 días	jue 28/08/25	vie 5/09/25	19
21		Definir estrategia de respuesta ante riesgos	5 días	lun 8/09/25	vie 12/09/25	20
22		Elaboración de declaración de aplicabilidad de los controles a implementar	10 días	lun 15/09/25	vie 26/09/25	21
23		FASE 2: HACER	130 días	jue 3/07/25	mié 31/12/25	
24		Definir estructura organizativa para la gestión de la seguridad de la información	7 días	jue 3/07/25	vie 11/07/25	
25		elaborar documentación requerida para el funcionamiento y mejora del SGSI	25 días	lun 14/07/25	vie 15/08/25	24
26		Elaborar procedimientos y mecanismos para realizar acciones correctivas y preventivas en el tratamiento de no conformidades	35 días	lun 18/08/25	vie 3/10/25	25
27		Documentar contoles de seguridad	25 días	lun 6/10/25	vie 7/11/25	26
28		Elaborar plan de revisión periodica de la politica y alcance del SGSI	10 días	lun 10/11/25	vie 21/11/25	27
29		Desarrollar plan de capacitación en el SGSI para personal de la JNJ	8 días	lun 24/11/25	mié 3/12/25	28
30		Desarrollar taller de capacitación en el SGSI para todo el personal de la JNJ	10 días	jue 4/12/25	mié 17/12/25	29
31		Realizar gestión de incidentes y operaciones del SGSI, elaboración de politica de gestion de incidentes de la JNJ	10 días	jue 18/12/25	mié 31/12/25	30
32		FASE 3: VERIFICAR	55 días	lun 5/01/26	vie 20/03/26	
33		Realizar una auditoria interna al SGSI implementado	15 días	lun 5/01/26	vie 23/01/26	
34		Formular plan de acción para levantamiento de no conformidades	7 días	lun 26/01/26	mar 3/02/26	33



Proyecto: Cronograma de imple
Fecha: mar 27/08/24

Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
35		Remitir recomendaciones para mejora del SGSI	7 días	mié 4/02/26	jue 12/02/26	34
36		Evaluar nivel de cumplimiento del SGSI post implementación	5 días	vie 13/02/26	jue 19/02/26	35
37		Coordinar revisión de alta dirección para aprobación del SGSI	7 días	vie 20/02/26	lun 2/03/26	36
38		Efectuar mejoras al SGSI en coordinación con alta dirección	7 días	mar 3/03/26	mié 11/03/26	37
39		Elaborar documentación para auditores internos de la entidad	7 días	jue 12/03/26	vie 20/03/26	38
40		FIN de implementación SGSI	1 día	vie 20/03/26	vie 20/03/26	
41		Contratar servicio de auditoria externa para revisión del SGSI de la JNJ	35 días	jue 2/04/26	mié 20/05/26	
42		Contratar servicio de levantamiento de no conformidades	30 días	jue 21/05/26	mié 1/07/26	41
43		Contratar servicio de certificación de subproceso de la DSN	25 días	jue 2/07/26	mié 5/08/26	42



Proyecto: Cronograma de imple
Fecha: mar 27/08/24

Tarea
División
Hito
Resumen
Resumen del proyecto
Tarea inactiva
Hito inactivo
Resumen inactivo
Tarea manual
solo duración
Informe de resumen manual
Resumen manual
solo el comienzo
solo fin
Tareas externas
Hito externo
Fecha límite
Progreso
Progreso manual