MANUAL DE PROCESOS Y PROCEDIMIENTOS DE OFICINA DE SEGURIDAD INFORMÁTICA

S06 GESTIÓN DE SEGURIDAD INTEGRAL, EMERGENCIAS Y DESASTRES

MANUAL DE PROCESOS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA
(VERSIÓN AS-IS)

GRADO	CARGO	NOMBRES Y APELLIDOS	FIRMA
Validado por	Gerente Central	Víctor German Chávez Bahamonde	
Validado por	Jefe de la Oficina de Seguridad Informática	Giuliana Helen Mantilla Montes	

HOJA DE CONTROL DE CAMBIOS

N°	ÍTEMS	DESCRIPCIÓN DEL CAMBIO	VERSIÓN	RESPONSABLE
01		Versión inicial del documento	v.1	Sub Gerencia de Procesos
02		Versión con Primera Actualización del documento	v.2	Sub Gerencia de Procesos

ÍNDICE

1. Objetivo

Crear un marco de referencia que reglamente la seguridad que debe darse a la información interna tomando como base las políticas y normas definidas. Dotar de una herramienta que le permita de manera clara y definida, dar cumplimiento a las políticas y normas relacionadas con la seguridad de la información

2. Alcance

El presente documento está dirigido a todo el personal de la Oficina de Seguridad Informática, involucrados en las actividades planificar, diseñar, implementar y evaluar las tecnologías de información y seguridad de la institución en el ámbito nacional.

3. Finalidad

Establecer lineamientos de trabajo para la Unidad de Informática con el fin seguir los procedimientos adecuados para proporcionar seguridad en el manejo y resguardo de información e infraestructura

4. Base legal

4.1 Ley N° 26790, Ley de Modernización de la Seguridad Social de Salud y sus modificatorias.

4.2 Ley N° 26790, Ley de Modernización de la Seguridad Social de Salud y sus modificatorias.

4.3 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y sus modificatorias.

4.4 Ley N° 27806, Ley de Transparencia y Acceso a la Información Púbica y sus modificatorias.

4.5 Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) y sus modificatorias.

4.6 Ley N° 28716, Ley de Control Interno de las Entidades del Estado.

4.7 Ley N° 29733, Ley de Protección de Datos Personales y sus modificatorias.

4.8 Ley N° 30096, Ley de Delitos Informática y sus modificatorias.

4.9 Decreto Supremo N° 009-1997-SA que aprueba el Reglamento de la Ley N° 26790, Ley de Modernización de la Seguridad Social de Salud.

4.10 Decreto Supremo Nº 030-2002-PCM, Reglamento de la Ley Marco de Modernización de la Gestión del Estado.

4.11 Decreto Supremo Nº 003-2013-JUS, que aprueba el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales.

4.12 Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.

4.13 Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital

4.14 Resolución de Contraloría N° 320-2006-CG, que aprueban Normas de Control Interno.

4.15 Resolución Jefatural N° 076-95-INEI, que aprueba la Directiva N° 007-95-INEI-SJI "Recomendaciones Técnicas para la Seguridad e Integridad de la Información que se procesa en la Administración Pública".

4.16 Resolución Jefatural N° 386-2002-INEI, que aprueba la Directiva N° 016-2002-INEI/DTNP, sobre Normas Técnicas para el almacenamiento y respaldo de la información procesada por las entidades de la administración pública.

4.17 Resolución Jefatural N° 088-2003-INEI, que aprueba la Directiva Nº 005-2003-INEI/DTNP, sobre "Normas para el uso del servicio de Correo Electrónico en las Entidades de la Administración Pública".

4.18 Resolución Ministerial N° 073-2004-PCM, que aprueba la "Guía para la Administración Eficiente de Software Legal en la Administración Pública".

4.19 Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de 06/07/2020 Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, 2 a Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

4.20 Resolución Ministerial N° 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.

4.21 Resolución Ministerial N° 087-2019-PCM, que aprueban disposiciones sobre conformación y funciones del Comité de Gobierno Digital

4.22 Resolución de Gerencia General N° 236-GG-ESSALUD-2005, que aprueba la Directiva de Gerencia General N° 002-GG-ESSALUD-2005, Políticas de Seguridad Informática de EsSalud, del 04 de mayo del 2005.

5. Vigencia

El presente manual tiene vigencia hasta el cambio de estructura y/o funciones de la Gerencia Central de Tecnologías de Información y Comunicaciones.

6. Definición y Términos

A continuación, se definen aquellos términos técnicos empleados en la descripción de los procesos que requieren aclaración de su significado:

Abreviaturas:

a. GCTIC: Gerencia Central de Tecnologías de Información y Comunicaciones
b. ESSALUD: Seguro Social de Salud
c. GCPP: Gerencia Central de Planeamiento y Presupuesto
d. GCAJ: Gerencia Central de Asesoría Jurídica
e. GCGP: Gerencia Central de Gestión de las Personas
f. FONAFE: Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado
g. SEGDI: Secretaria de Gobierno Digital
h. VB: Visto Bueno
i. IPRESS: Institución Prestadoras de Servicios de Salud
j. SGP-PCM: Secretaría de Gestión Pública de la Presidencia de Consejo de Ministros
k. TDR: Términos de Referencia
l. OSI: Oficina de Seguridad Informática
m. SIS: Seguro Integral de ESSALUD
n. SUSALUD: Superintendencia Nacional de Salud
o. ONP: Oficina de Normalización Previsional
p. SCTR: Seguro Complementario de Trabajo de Riesgo
q. ESSALUD: Seguro Social de Salud
r. APP: Asociación Público Privada
s. PCM: Presidencia de Consejo de Ministros
t. SI: Seguridad de la Información

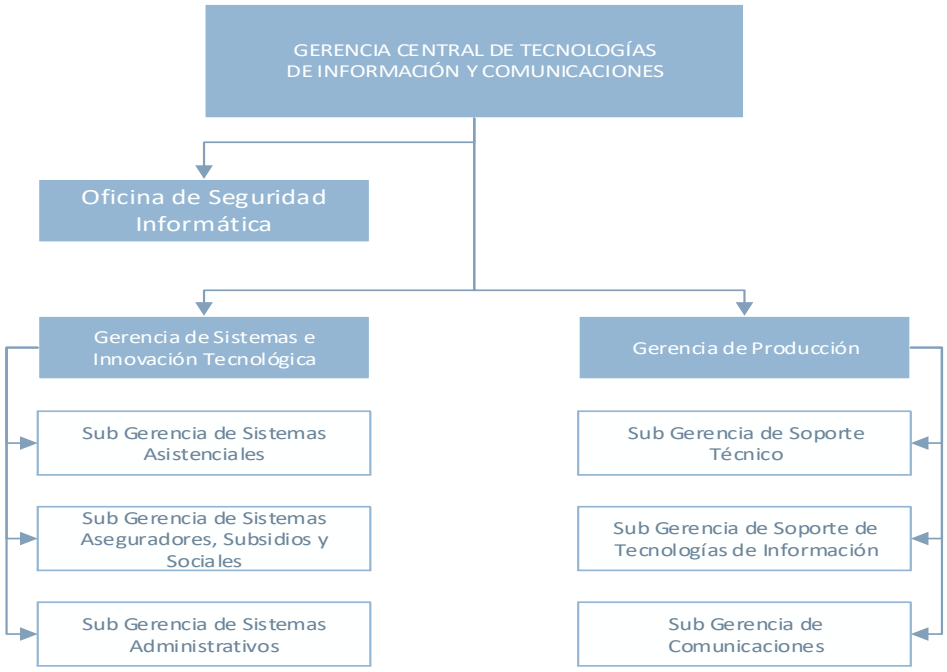
Definiciones y Términos:

a. **Cliente Interno:** Es el destinatario de los bienes y servicios, que puede ser una persona, grupo, entidad, empresa, entre otros al interior del proceso que recibe un bien y servicio.
b. **Cliente externo:** Es el destinatario de los bienes y servicios, que puede ser una persona, grupo, entidad, empresa, entre otros al externo del proceso que recibe un bien y servicio.
c. **Actividad:** Tarea o conjunto de tareas necesarios para realizar un proceso.

d. **Bien o servicio:** Es el resultado de un proceso.
e. **Diagrama de Flujo:** Es una representación con imágenes de las actividades de un proceso, útil para investigar las oportunidades de mejora, al obtener un conocimiento detallado del modo real de funcionamiento del proceso en ese momento.
f. **Contratista**: Postor ganador de la buena pro que celebra un contrato con una entidad, de conformidad con las disposiciones de la Ley de Contrataciones del estado y de su reglamento.
g. **Especificaciones Técnicas (EETT):** Descripción de las características técnicas y/o requisitos funcionales del bien a ser contratado. Incluye las cantidades, calidades y las condiciones bajo las que debe ejecutarse las obligaciones.
h. **Hardening:** Es el proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuanto más funciones desempeña.
i. **Kick Off de Proyecto:** Es la reunión que determina el inicio de un proyecto, la primera toma de contacto entre los clientes y los empleados.
j. **Mapa de procesos:** Representación gráfica de la secuencia e interacción de los diferentes procesos que tiene lugar en una entidad.
k. **Procesos:** Conjunto de actividades mutuamente interrelacionadas o que interactúen, las cuales transforman elementos de entrada en resultados.
l. **Procesos de Nivel 0:** Usualmente se utiliza el término de Macro proceso para denominar grupos de procesos.
m. **Procesos de Nivel 1:** Primer nivel de desagregación de un Proceso de Nivel 0.
n. **Procesos de Nivel 2:** Segundo nivel de desagregación de un Proceso de Nivel 0.
o. **Procesos de Nivel N:** Último nivel de desagregación de un Proceso de Nivel 0. Se describe a través de procedimientos que lo conforman.
p. **Procedimientos:** Es la descripción de forma específica y detallada del ultimo nivel desagregado del proceso, de cómo se lleva a cabo. Son las instrucciones, pautas, pasos que describen la forma de ejecutar un proceso Nivel N-
q. **Producto:** Bien o servicio creado por el proceso.
r. **Proveedor:** Entidad o persona que proporciona un bien y servicio.
s. **Implementación:** Proceso que consiste en poner en ejecución la norma aprobada, lo cual implica que las normas, reglas o lineamientos, criterios, metodologías y procedimientos consignadas en las misma se apliquen.

7. Consideraciones

El presente Manual comprende las actividades que son de responsabilidad de la Oficina de Seguridad Informática, considerando que su organización está dada de la siguiente manera:



7.1 El presente Manual de Procesos y Procedimientos de la Oficina de Seguridad Informática está sujeto a modificaciones y/o actualizaciones, debido a que constantemente se realizan mejoras en los procesos a fin de dar la eficiente gestión institucional en pro de la satisfacción del usuario.

7.2 El presente Manual de Procesos y Procedimientos se ha diseñado en base a la Metodología de la Presidencia de Consejo de Ministros (PCM), Resolución de Secretaría de Gestión Pública N° 006- 2018-PCM/SGP, que aprueba la Norma Técnica N° 001-2018-SGP, Norma Técnica para la implementación de la gestión por procesos en las entidades de la administración pública.

8. Aspectos Generales

8.1 Alineamiento de los procesos con el mapa de procesos nivel 0 y objetivos estratégicos y operativos

OBJETIVO ESTRATEGICO PEI 20120-2024		ACCIONES ESTRATÉGICAS INSTITUCIONALES		MACRO-PROCESO VINCULADO	INDICADOR DE ALINEAMIENTO
OEI. 01	Proteger Financieramente las Prestaciones que se brindan a los Asegurados garantizando una gestión eficiente de los recursos	AEI. 1.1	Gestión oportuna y eficiente de los recursos para financiar los servicios institucionales	E01 Gestión de Planificación Estratégica	Ratio de deuda respecto al Presupuesto
				M01 Gestión de Aseguramiento en Salud	Índice de siniestralidad por tipo de Seguro
				S02 Gestión Financiera	Variación de la tasa de retorno de inversiones financieras respecto al periodo anterior
				E03 Gestión de Riesgos	
				S01 Gestión Logística	Porcentaje de dispensación de medicamentos respecto al total prescrito
				M02 Prestaciones de Salud	
				E04 Gestión de Calidad	Variación del gasto asistencial de las personas atendidas en situación de afiliación indebida o por fuera de su cobertura de salud
				E02 Modernización	
				M03 Prestaciones Sociales	
				M04 Prestaciones Económicas	
		AEI. 1.2	Manejo eficiente de los gastos institucionales		Porcentaje de Gasto administrativo respecto al Presupuesto total
				E06 Control Interno	

OEI.02	Brindar a los asegurados acceso oportuno a prestaciones integrales y de calidad acorde a sus necesidades	AEI. 2.1	Mejorar el modelo de atención integral diferenciado por ciclo de vida, con asegurados empoderados en sus derechos y deberes	M02 Prestaciones de Salud	Satisfacción del usuario
				M03 Prestaciones Sociales	Porcentaje de cumplimiento de la cartera de servicios preventivos según norma técnica o protocolo nacional establecido
				M04 Prestaciones Económicas	Porcentaje de cumplimiento de adherencia alta a las recomendaciones de las Guías de Práctica Clínica (GPC) o protocolo establecido
		AEI. 2.2	Estándares de calidad alineados a las expectativas y necesidades de los asegurados	M01 Gestión de Aseguramiento en Salud	Diferimiento en Consulta Externa en centros asistenciales del primer nivel
				S04 Gestión Jurídica	
				E04 Gestión de Calidad	Adherencia al registro de eventos relacionados a la seguridad del paciente
				E02 Modernización	
		AEI. 2.3	Articulación efectiva de la red inter e intrainstitucional al servicio del asegurado		Porcentaje de atenciones de emergencia de prioridad IV y V
				E03 Gestión de Riesgos	Porcentaje de referencia no pertinentes
					Porcentaje de Contra-referencias
				S02 Gestión Financiera	Diferimiento de citas en procedimientos de apoyo al diagnóstico en Radiología y Ecografía
		AEI. 2.4	Servicios disponibles para brindar atenciones con oportunidad y calidad a los asegurados	S01 Gestión Logística	
				S08 Gestión de Proyectos de Inversión	Porcentaje de equipamiento operativo de Resonador, Tomógrafo, Equipo de Rayos X, Ecógrafo, Endoscopio
				S07 Gestión de Tecnologías de Información y comunicación	
		AEI. 2.5	Recurso humano disponible, competente y eficientemente distribuido	S03 Gestión de Capital Humano	Porcentaje de personal evaluado
					Ratio médico x10000 asegurados
				E01 Gestión de Planificación Estratégica	Porcentaje de ausentismo laboral (en horas)
		AEI. 2.6	Prevención de la vulnerabilidad y gestión de desastres	S06 Gestión de Seguridad Integral, Emergencias y desastres	Porcentaje de riesgos en IPRESS de mayor vulnerabilidad
				E06 Control Interno	

OEI.03	Impulsar la transformación digital y la gestión para resultados centrada en los asegurados logrando modernizar la institución	AEI. 3.1	Implementación de procesos para la separación de funciones según la Ley AUS	E01 Gestión de Planificación Estratégica	Porcentaje de procesos implementados en el marco de la separación de funciones
				E02 Modernización	Porcentaje de sistemas clave interoperables
		AEI 3.2	Implementación de Sistemas Interoperables, que brinden información confiable y oportuna para tomar decisiones en la institución	S07 Gestión de Tecnologías de Información y comunicación	Porcentaje de procesos que son soportados por sistemas clave interoperables
				S08 Gestión de Proyectos de Inversión	Porcentaje de aplicativos implementados en nube
				S05 Gestión Documental	
		AEI 3.3	Gestión institucional articulada con enfoque de resultados y centrada en el asegurado	M01 Gestión de Aseguramiento en Salud	Ratio de indicadores clave de gestión obtenidos por algoritmos automatizados, en los Procesos misionales
				E05 Gestión de Imagen Institucional	
				E06 Control Interno	Índice de percepción de buen trato en los servicios
				E04 Gestión de Calidad	
		AEI 3.4	Desempeño ético y empático de los colaboradores en la institución	S03 Gestión de Capital Humano	Índice de clima laboral
				E03 Gestión de Riesgos	

8.2 Matriz Cliente Producto

Cliente / Producto		Operaciones del SGSI	Políticas de Seguridad de la Información	Cumplimiento de Controles	Continuidad Operacional	Visitas Inopinadas y Capacitación	Gestión de Riesgos de Seguridad de la Información	Gestión de la Seguridad Informática
Interno	Órganos de Alta Dirección	X	X	X	X	X	X	X
	Órgano de Control	X	X	X	X	X	X	X
	Órganos de Apoyo y Asesoramiento de la Alta Dirección	X	X	X	X	X	X	X
	Órganos de Administración Interna - Asesoramiento	X	X	X	X	X	X	X
	Órganos de Administración Interna - Apoyo	X	X	X	X	X	X	X
Interno	Órganos de Línea	X	X	X	X	X	X	X
	Órganos Desconcentrados	X	X	X	X	X	X	X
	Órganos Prestadores Nacionales	X	X	X	X	X	X	X
Externo	Asociación Público Privada (APP)			X	X	X	X	X

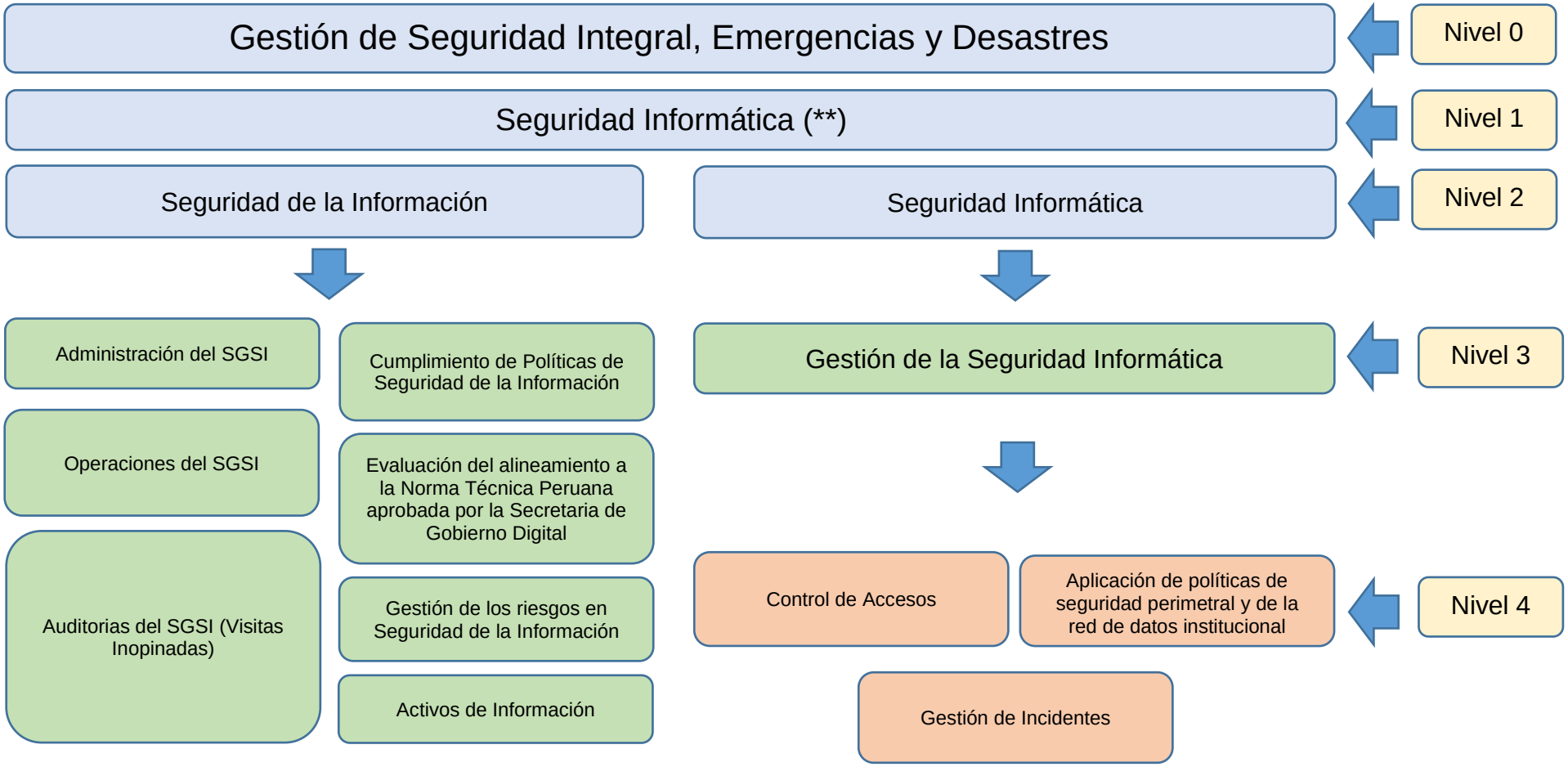
Cliente / Producto		Operaciones del SGSI	Políticas de Seguridad de la Información	Cumplimiento de Controles	Continuidad Operacional	Visitas Inopinadas y Capacitación	Gestión de Riesgos de Seguridad de la Información	Gestión de la Seguridad Informática
	Entidades del estado con los cuales se cuenta con un contrato y/o convenio (RENIEC, SUNAT, MINSA, MAC)			X	X	X	X	X
	Entidades privadas con los cuales se encuentra un contrato vigente (Proveedores)			X	X	X	X	X

8.3 Matriz de Responsabilidad

PROCESOS PRINCIPALES (**)										
Macro Procesos / Oficinas	**S06.01.01.01** Administración del SGSI	**S06.01.01.02** Operaciones del SGSI	**S06.01.01.03** Auditorias del SGSI (Visitas Inopinadas)	**S06.01.01.04** Cumplimiento de Políticas de Seguridad de la Información	**S06.01.01.05** Evaluación del alineamiento a la Norma Técnica Peruana aprobada por la Secretaria de Gobierno Digital	**S06.01.01.06** Gestión de los riesgos en Seguridad de la Información	**S06.01.01.07** Activos de Información	**S06.01.02.02.08** Control de Accesos	**S06.01.02.02.09** Aplicación de políticas de seguridad perimetral	**S06.01.02.02.10** Actualización de software de los equipos de seguridad
Gerencia Central de Tecnologías de Información y Comunicaciones	A	A	A	A	A	A	A	A	A	A
Oficina de Seguridad Informática	R	R	R	R	R	R	R	CI	CI	CI
Gerencia de Sistemas e Innovación Tecnológica	I	I	I	I	I	I	I	I	I	I
Gerencia de Producción								R	R	R

R: Responsible / Responsable. Es el que se encarga de hacer la tarea o actividad.
A: Accountable / Persona a cargo. Es la persona que es responsable de que la tarea esté hecha. No es lo mismo que la R, ya que no tiene porqué ser quien realiza la tarea, puede delegarlo en otros. Sin embargo, si es quien debe asegurarse de que la tarea se haga, y se haga bien.
C: Consulted / Consultor. Los recursos con este rol son las personas con las que hay que consultar datos o decisiones con respecto a la actividad o proceso que se define.
I: Informed / Informar. A estas personas se las informa de las decisiones que se toman, resultados que se producen, estados del servicio, grados de ejecución, etc.

8.4 Diagrama de Bloques



9. Aspectos Específicos

9.1 Inventario de los procesos (**)

Código	Denominación del Proceso	Código	Denominación del Proceso	Código	Denominación del Proceso	Código	Denominación del Proceso	Código	Denominación del Proceso
Nivel 0	Nivel 0	Nivel 1	Nivel 1	Nivel 2	Nivel 2	Nivel 3	Nivel 3	Nivel 4	Nivel 4
S06	Gestión de Seguridad Integral, Emergencias y Desastres	S06.01	Gestión de Seguridad Informática	S06.01.01	Seguridad de la Información	S06.01.01.01	Administración del SGSI		
						S06.01.01.02	Operaciones del SGSI		
						S06.01.01.03	Auditorias del SGSI (Visitas Inopinadas)		
						S06.01.01.04	Cumplimiento de Políticas de Seguridad de la Información		
						S06.01.01.05	Evaluación del alineamiento a la Norma Técnica Peruana aprobada por la secretaria de Gobierno Digital		
						S06.01.01.06	Gestión de los riesgos en Seguridad de la Información		
						S06.01.01.07	Activos de Información		
				S06.01.02	Seguridad Informática	S06.01.02.01	Gestión de la Seguridad informática	S06.01.02.01.01	Control de Accesos
								S06.01.02.01.02	Aplicación de políticas de seguridad perimetral y de la red de datos institucional.
								S06.01.02.02.03	Gestión de incidentes

9.2 Ficha de Procesos de Nivel 01, 02 hasta el nivel N

9.2.1 Ficha de Nivel 01: S06.01 Seguridad Informática (**)

Nombre	Seguridad Informática
Objetivo	Garantizar el cumplimiento de un nivel adecuado de seguridad de información en la institución.
Descripción	▪ Establecer lineamientos de seguridad de información en la institución e implementar el SGSI (Sistema de Gestión de Seguridad de Información) en EsSalud, con la finalidad de lograr la madurez de los controles de seguridad de información en la institución, alineados a la Ley de Gobierno Digital. ▪ Gestionar la Seguridad Informática de acuerdo a los lineamientos de seguridad de información y que apliquen a todos los procesos (asistenciales, administrativos, etc.), tecnologías y al personal labora en EsSalud bajo las distintas modalidades.
Alcance	Gerencia Central de Tecnologías de Información y Comunicaciones, Redes Asistenciales

Proveedor	**Entrada**	**Listado de Procesos de Nivel 2**	**Salidas**	**Destinatario de los bienes y servicios**
- Normas ISO internacionales / INACAL - PCM, Grupos de trabajo (Seguridad de Información), Foros Nacionales e Internacionales, Proveedores de SI - ISO Internacional, INACAL - Gerencia de Producción - Personal interno OSI Gerencia Central de Finanzas	- Adquisición ISO 31000 o su equivalente en la NTP - Adquisición ISO 27005 o su equivalente en la NTP - Incidentes de seguridad Norma Técnica Peruana Resoluciones de PCM Leyes - Realizar programación anual de los lugares a ser visitados - Presupuesto para realizar Visitas de Cumplimiento	Seguridad de la Información	-Reporte de Cumplimiento de Políticas de Seguridad de Información. -Visitas inopinadas/Evaluaciones de seguridad de información. -Plan del Sistema de Gestión de Seguridad de Información	- EsSalud, Postores y Proveedores - Usuarios internos y externos que utilizan los Sistemas de EsSalud - EsSalud, Postores y Proveedores
		Seguridad Informática	Reportes técnicos de seguridad informática en la Gestión de Cambios, Control de Accesos, Seguridad Perimetral y Gestión de Incidencias	

Indicadores	(Número de documentos presentados a GCTIC / Total de documentos planificados)*100 (Número de Visitas realizadas / Número de Visitas planificadas)*100 (Número de Indicadores totales / Numero de Indicadores Periodo anterior)*100 (Número de Normas revisadas / Total de Normas actualizadas)*100 (Número de Normas aprobadas / Total de Normas difundidas a nivel nacional)*100 (Número de Tipos de Incidentes de seguridad de información documentados / Total de Tipos de Incidentes)*100 (Número de pases a producción con visto bueno / Total de pases a producción solicitados)*100 (Cantidad de accesos que cumplen las políticas de SI / Cantidad de accesos brindados al proveedor)*100 (Cantidad de configuraciones o reglas realizadas / Cantidad de configuraciones o reglas solicitadas)*100
Registros	Solicitud de acceso Cronograma de actividades Cronograma de trabajo Plan de actividades Ticket de atención Correo electrónico Listado de actividades realizadas Informe de realización de actividades
Elaborado por:	Oficina de Seguridad Informática Gerencia de Producción
Revisado por:	Subgerencia de Comunicaciones Oficina de Seguridad Informática Gerencia de Producción
Aprobado por:	Gerencia Central de Tecnologías de Información y Comunicaciones

9.2.2 Ficha de Nivel 02: S06.01.01 Seguridad de la Información

Nombre	Seguridad de la Información (**)
Objetivo	Establecer lineamientos de seguridad de información en la institución e implementar el SGSI (Sistema de Gestión de Seguridad de Información) en EsSalud, con la finalidad de lograr la madurez de los controles de seguridad de información en la institución, alineados a la Ley de Gobierno Digital.
Descripción	Establecer lineamientos de seguridad de información en la institución e implementar el SGSI (Sistema de Gestión de Seguridad de Información) en EsSalud, con la finalidad de lograr la madurez de los controles de seguridad de información en la institución, alineados a la Ley de Gobierno Digital y a las NTPs vigentes de obligatorio cumplimiento establecido por la Secretaria de Gobierno Digital de la PCM.
Alcance	Gerencia Central de Tecnologías de Información y Comunicaciones, Redes Asistenciales

Proveedor	Entrada	Listado de Procesos de Nivel 3	Salidas	Destinatario de los bienes y servicios
- Presidencia de Consejos de Ministros - Oficina de Control Institucional - Normas ISO internacionales - INACAL	- Documentos de SEDGI, OCI, NTP, auditoría externa	Administración del SGSI	- Políticas de Seguridad de la - Información Plan de SGSI - Normativa sobre Protección de Datos Personales - Metodología de Riesgos escogida para utilizarla en EsSalud	- Usuarios internos y externos que utilizan los Sistemas de EsSalud
- Oficina de Seguridad Informática	'- Documentos normativos aprobados	Operaciones del SGSI	- Informe de incidentes de SI - Informe de vulnerabilidades - informe de evaluación de herramientas de SI - Informe de evaluación de los servicios de las herramientas SI - Informe de impacto comercial - Informe de Diseño y Arquitectura de sistemas y/o aplicaciones - Gestión de Riesgos de Seguridad de la Información	- Gerencia Central de Tecnologías de Información y Comunicaciones - Redes asistenciales a nivel nacional
- Oficina de Seguridad Informática	- Listado de visitas a la Redes Asistenciales de EsSalud	Auditorias del SGSI (Visitas Inopinadas)	- Programación de planes de auditoria y supervisión	- Gerente de Red, Personal de la Red Asistencial y Administrativo

- Profesional de la Seguridad de la Información			- Informe técnico de visita - Rendición de cuentas	
- Oficina de Seguridad Informática	- Documentos referidos a la seguridad de información Solicitud de consulta sobre procedimientos de seguridad de información	Cumplimiento de Políticas de Seguridad de la Información	- Planes de Acción de Auditoria de la OSI - Matriz de Activos - Plan de Acción de la Ley de Protección de Datos	- Comité de Gobierno Digital - Gerencia Central de Tecnologías de Información y Comunicaciones - Jefe de OSI a Nivel Nacional - Profesionales de Seguridad de la Información
- Presidencia de Consejos de Ministros - Oficina de Seguridad Informática	- Norma Técnica Peruana	Evaluación del alineamiento a la Norma Técnica Peruana aprobada por la Secretaria de Gobierno Digital	- Documentos normativos modificados	Todas las áreas de EsSalud, Postores, Proveedores
- Profesional de Seguridad de la Información - Usuario de EsSalud	- Herramientas de seguridad - Identificación del riesgo de seguridad - Documentos de tratamiento de eventos relacionados al marco de la seguridad y privacidad	Gestión de los riesgos en Seguridad de la Información	- Documentos de control de mitigación de riesgo de seguridad	- Oficina de Seguridad Informática EsSalud - Gerencia de Producción - Gerencia Central de Tecnologías de Información y Comunicaciones
- Oficina de Seguridad Informática EsSalud - Usuario de EsSalud a Nivel Nacional	- Documentos de clasificación de activos – Documento de criticidad y aplicabilidad de activos de información críticos	Activos de información	- Documentos de control de Clasificación y criticidad de activos de información	- Gerencia Central de Tecnologías de Información y Comunicaciones - Usuarios internos y externos que utilizan los activos de información de EsSalud
Indicadores	(Número total de Informes técnicos del SGSI / Total de Informes técnicos de la OSI) *100 (Número total de Normas elaboradas / Total de normas aprobadas y difundidas a nivel nacional) *100 (Número de informes de metodología PDCA aplicada del SGSI / Total de Informes Técnicos de la OSI) *100 (Número de Documentos presentados a OSI / Total de documentos planificados) *100 (Número de visitas inopinadas planificadas / Número de visitas inopinadas realizadas) *100 (Número de Informes elaborados para la GCTIC / Número de informes presentados a la GCTIC) *100 (Número de Indicadores totales / Numero de Indicadores Periodo anterior) *100 (Número de Normas revisadas / Total de Normas actualizadas) *100			

	(Número de Tipos de Incidentes documentados / Total de Tipos de Incidentes) *100 (Número de estadísticas implementadas de control de cumplimiento de la normativa vigente / Número de estadísticas establecidas de control de cumplimiento de la normativa vigente) *100 (Número total de lineamientos aplicados / Total de lineamientos dispuestos por la Ley de Protección de Datos Personales) *100 (Número de activos de información identificados / Total de activos de información clasificados) *100
Registros	Documentos, informes, correos
Elaborado por:	Personal de Seguridad de la Información
Revisado por:	Oficina de Seguridad Informática
Aprobado por:	Gerencia Central de Tecnologías de Información y Comunicaciones

9.2.3 Ficha de Nivel 02: S06.01.02 Seguridad Informática

Nombre	Seguridad Informática (**)
Objetivo	Gestionar la Seguridad Informática de acuerdo con los lineamientos de seguridad de información y que apliquen a todos los procesos (asistenciales, administrativos, etc.), tecnologías y al personal labora en EsSalud bajo las distintas modalidades.
Descripción	Aplicar las buenas prácticas en Seguridad de Información para una correcta administración de los equipos
Alcance	Gerencia Central de Tecnologías de Información y Comunicaciones

Proveedor	Entrada	Listado de Procesos de Nivel 3	Salidas	Destinatario de los bienes y servicios
- Normas ISO internacionales / INACAL - PCM, Grupos de trabajo (Seguridad de Información), Foros Nacionales e Internacionales, Proveedores de SI - Unidades orgánicas de EsSalud	- Requerimiento - Contrato de proveedores - Reportes de vulnerabilidad - Informes del área responsable de los servicios de operación	Gestión de la Seguridad Informática	- Supervisión de las herramientas de seguridad - Evaluación de aplicabilidad de controles y procesos formales de accesos aplicados por los servicios de operación - Evaluación de los procesos normados en el control de accesos - Evaluación de la aplicabilidad de las políticas de seguridad de la información - Informe de incidentes de SI - Informe de vulnerabilidades - Informe de evaluación de herramientas de SI - Informe de evaluación de los servicios de las herramientas SI - Informe de impacto comercial - Informe de Diseño y Arquitectura de sistemas y/o aplicaciones - Gestión de Riesgos de Seguridad de la Información. (Del numeral 9.2.2 Ficha de Nivel 02: S06.01.01 Seguridad de la Información).	Unidades orgánicas de EsSalud Redes asistenciales Redes prestacionales Proveedores Asegurados

Indicadores	(Cantidad de accesos cerrados / Cantidad de accesos brindados al proveedor) *100 (Cantidad de políticas y controles / Cantidad de políticas y controles aplicados) *100 (Cantidad de incidentes reportados / Cantidad de incidentes resueltos) *100
Registros	Solicitud de acceso Cronograma de actividades Cronograma de trabajo Plan de actividades Ticket de atención Correo electrónico Listado de actividades realizadas Informe de realización de actividades Consolidados de formularios atendidos Solicitud de acceso Informe de controles normativos aplicados Términos de referencia alineadas a la NTP 27001 Especificaciones técnicas alineadas a la NTP 27001 Plan de Roll Back Plan de Backup Registro de altas y bajas de accesos
Elaborado por:	Gerencia de Producción
Revisado por:	Subgerencia de Comunicaciones Oficina de Seguridad Informática Gerencia de Producción
Aprobado por:	Gerencia Central de Tecnologías de Información y Comunicaciones

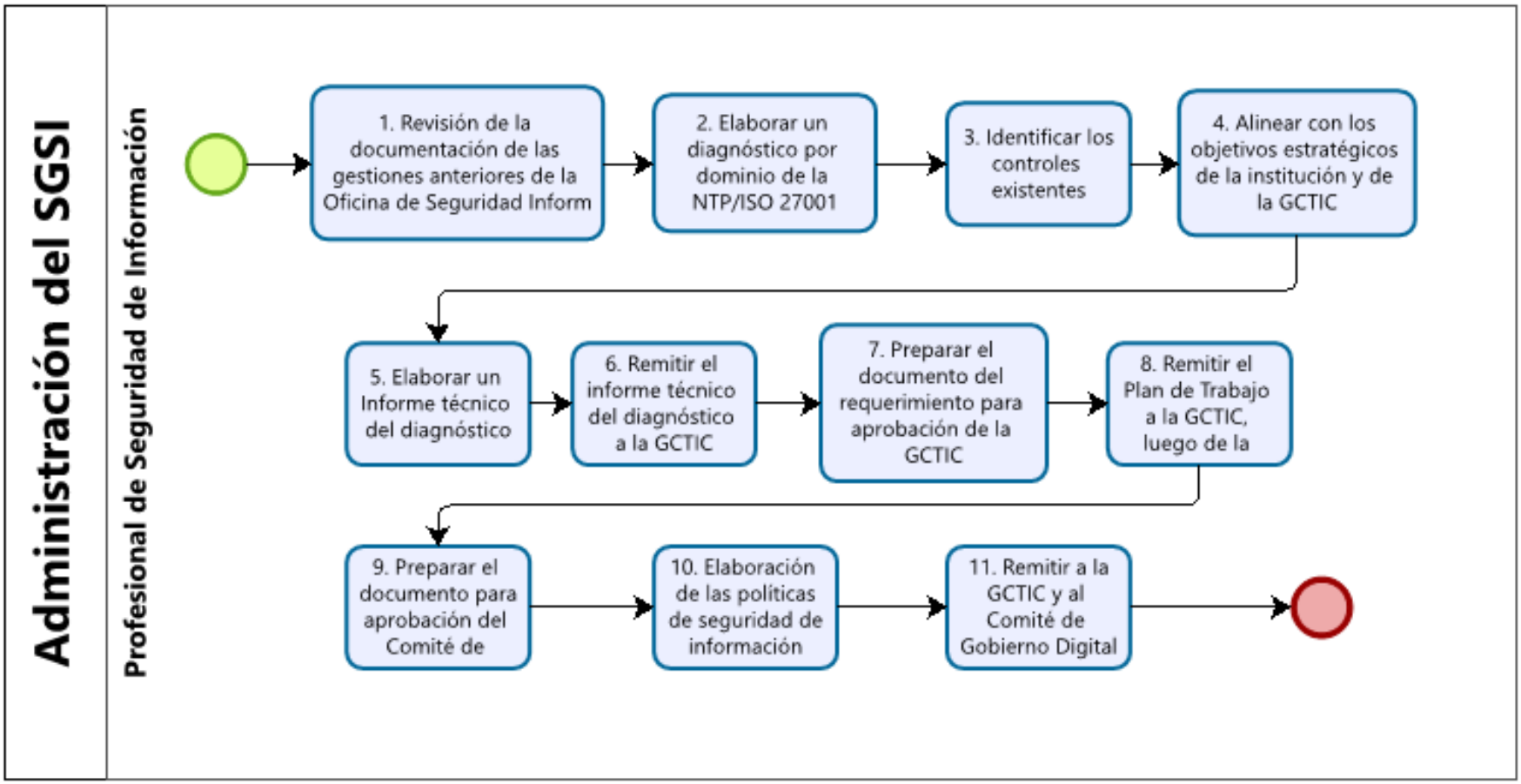
9.2.4 Ficha de Nivel 03: S06.01.02.01 Gestión de la Seguridad Informática

<table>
<tr><td>Nombre</td><td colspan="4">Gestión de la Seguridad Informática (**)</td></tr>
<tr><td>Objetivo</td><td colspan="4">Establecer los criterios de control, seguimiento y verificación de cumplimiento a todas las actividades que se realicen durante la administración de los equipos de seguridad perimetral</td></tr>
<tr><td>Descripción</td><td colspan="4">Aplicar las buenas prácticas en Seguridad de Información para una correcta administración de los equipos de seguridad perimetral</td></tr>
<tr><td>Alcance</td><td colspan="4">Gerencia Central de Tecnologías de Información y Comunicaciones</td></tr>
<tr><td>Proveedor</td><td>Entrada</td><td>Listado de Procesos de Nivel 4</td><td>Salidas</td><td>Destinatario de los bienes y servicios</td></tr>
<tr><td rowspan="3">- Normas ISO internacionales / INACAL
- PCM, Grupos de trabajo (Seguridad de Información), Foros Nacionales e Internacionales, Proveedores de SI
- Unidades orgánicas de EsSalud</td><td>- Informes del área responsable de atenciones críticas de acceso a operación
- Informes consolidado del área responsable de los servicios de operación</td><td>Control de Acceso</td><td>- Formulario de cambio por cada herramienta de seguridad.
- Formulario de acceso a base de datos.
- Formulario de acceso a servicios.
- Formulario de acceso para entidades externas.
- Formulario de solicitud de cuentas VPN SSL e IPsec
- Formato de Aceptación de Riesgos</td><td rowspan="3">- Unidades orgánicas de EsSalud
- Redes asistenciales
- Redes prestacionales
- Proveedores
- Asegurados</td></tr>
<tr><td>- Informes del área responsable de los servicios de operación por cumplimiento de controles</td><td>Aplicación de políticas de seguridad perimetral y de la red de datos institucional</td><td>- Informe de controles normativos aplicados alineados a las NTP 27001:2014
- Informe de cumplimiento de controles aplicados a la operación de herramientas de seguridad.
- Formato de Aceptación de Riesgos</td></tr>
<tr><td>- Planes de implementación y migración
- Contrato de proveedores
- Reportes de vulnerabilidad</td><td>Gestión de incidentes</td><td>- Plan de actividades
- Plan de Roll Back
- Plan de Backup
- Evaluación de impacto potencial en los servicios
- Formato de Aceptación de Riesgos</td></tr>
<tr><td>Indicadores</td><td colspan="4">(Cantidad de accesos cerrados / Cantidad de accesos brindados al proveedor) *100
(Cantidad de políticas y controles / Cantidad de políticas y controles aplicados) *100
(Cantidad de incidentes reportados / Cantidad de incidentes resueltos) *100</td></tr>
</table>

Registros	Consolidados de formularios atendidos Solicitud de acceso Informe de controles normativos aplicados Términos de referencia alineadas a la NTP 27001 Especificaciones técnicas alineadas a la NTP 27001 Cronograma de actividades Cronograma de trabajo Plan de actividades Plan de Roll Back Plan de Backup Registro de altas y bajas de accesos Ticket de atención Correos electrónicos Listado de actividades realizadas Informe y planes de realización de actividades
Elaborado por:	Gerencia de Producción
Revisado por:	Subgerencia de Comunicaciones Oficina de Seguridad Informática Gerencia de Producción
Aprobado por:	Gerencia Central de Tecnologías de Información y Comunicaciones

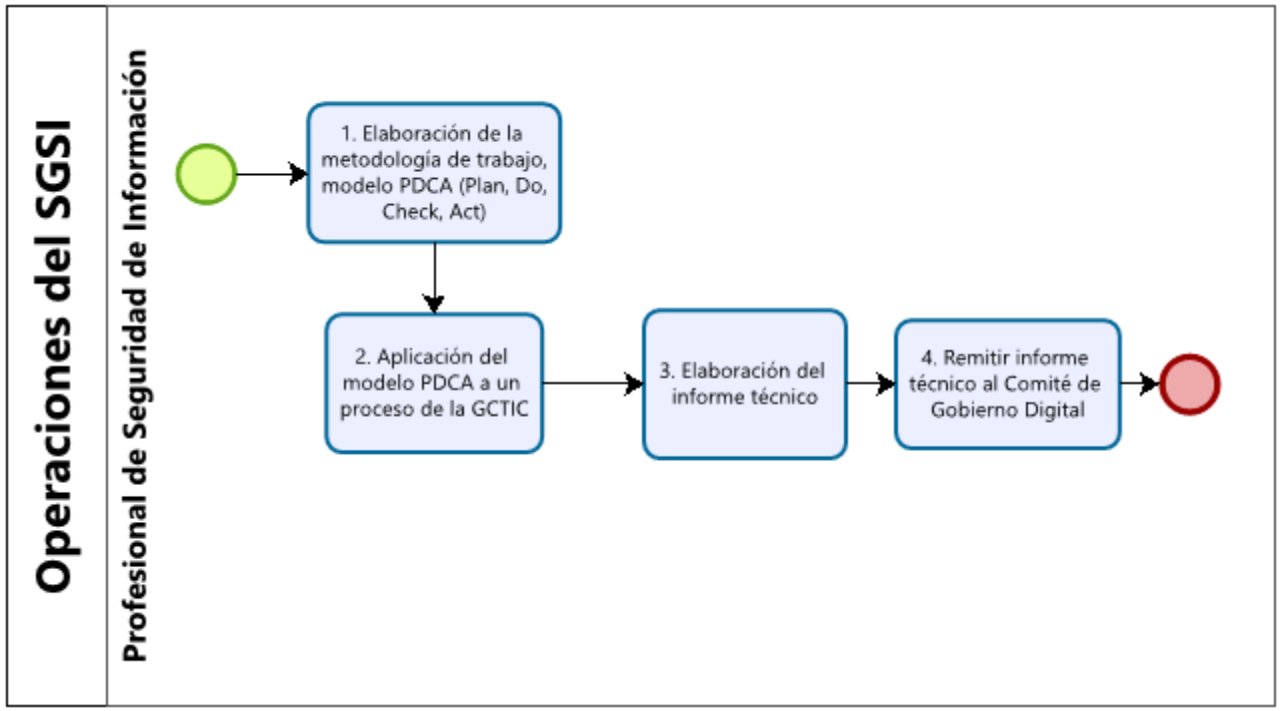
9.3 Modelado de procesos

S06.01.01.01 Administración del SGSI (**)

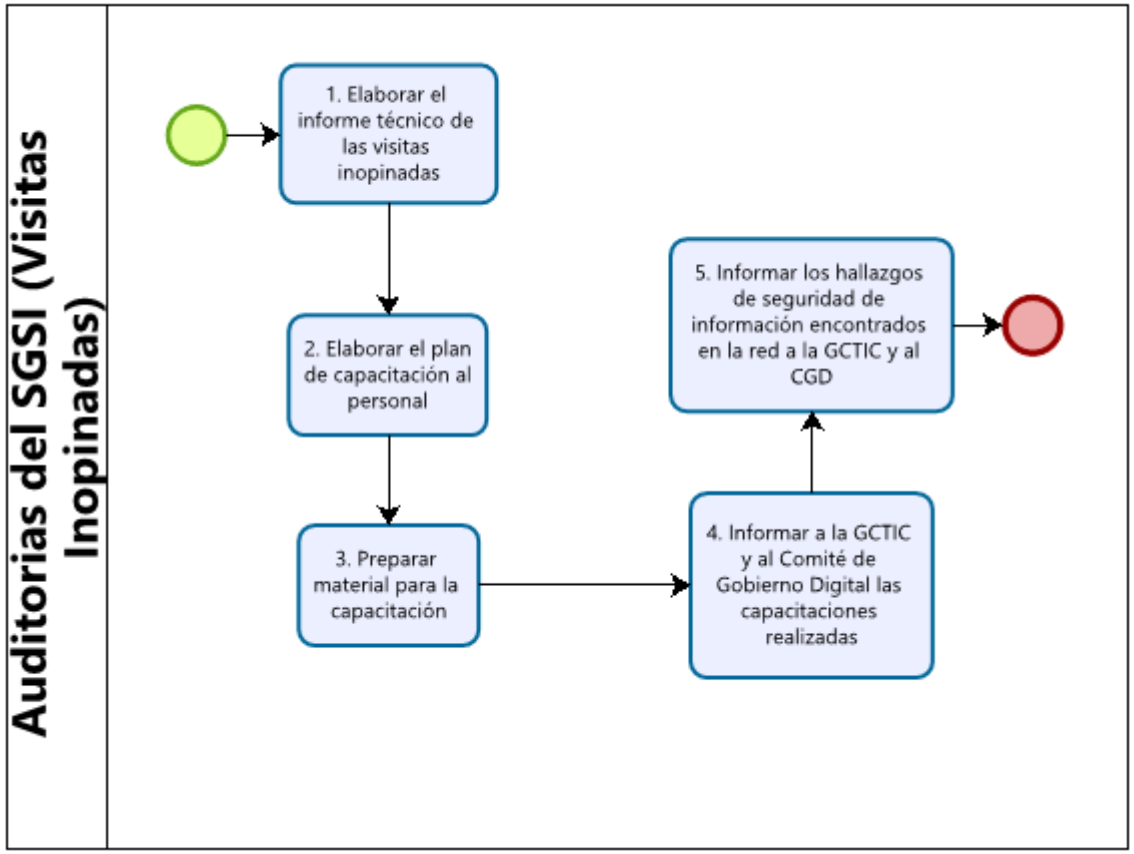


*** Al referirnos "Seguridad Informática" es a nivel de proceso, la gestión misma de la materia. De la misma forma, para Seguridad de Información. Ambos procesos registrados en el manual vienen ajustándose por la Oficina de Seguridad Informática de la GCTIC desde Julio del 2021 en base a los requerido en la NTP ISO/IEC 27001:2014.*

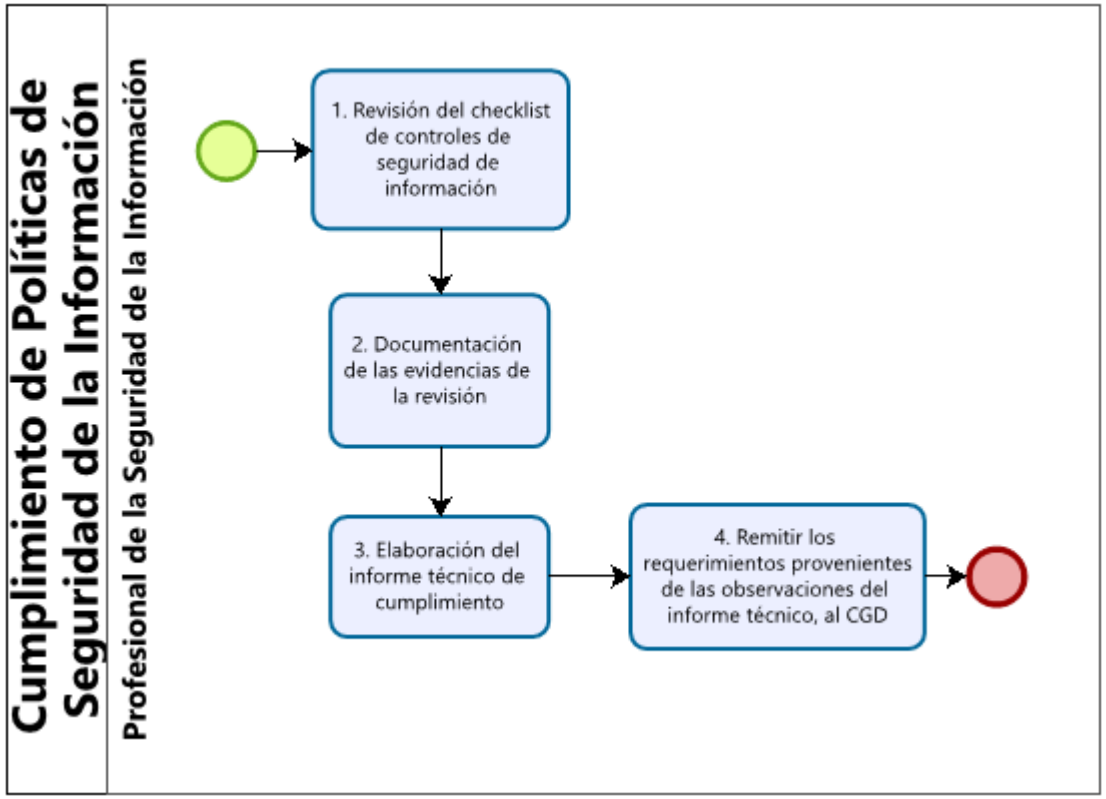
S06.01.01.02 Operaciones del SGSI



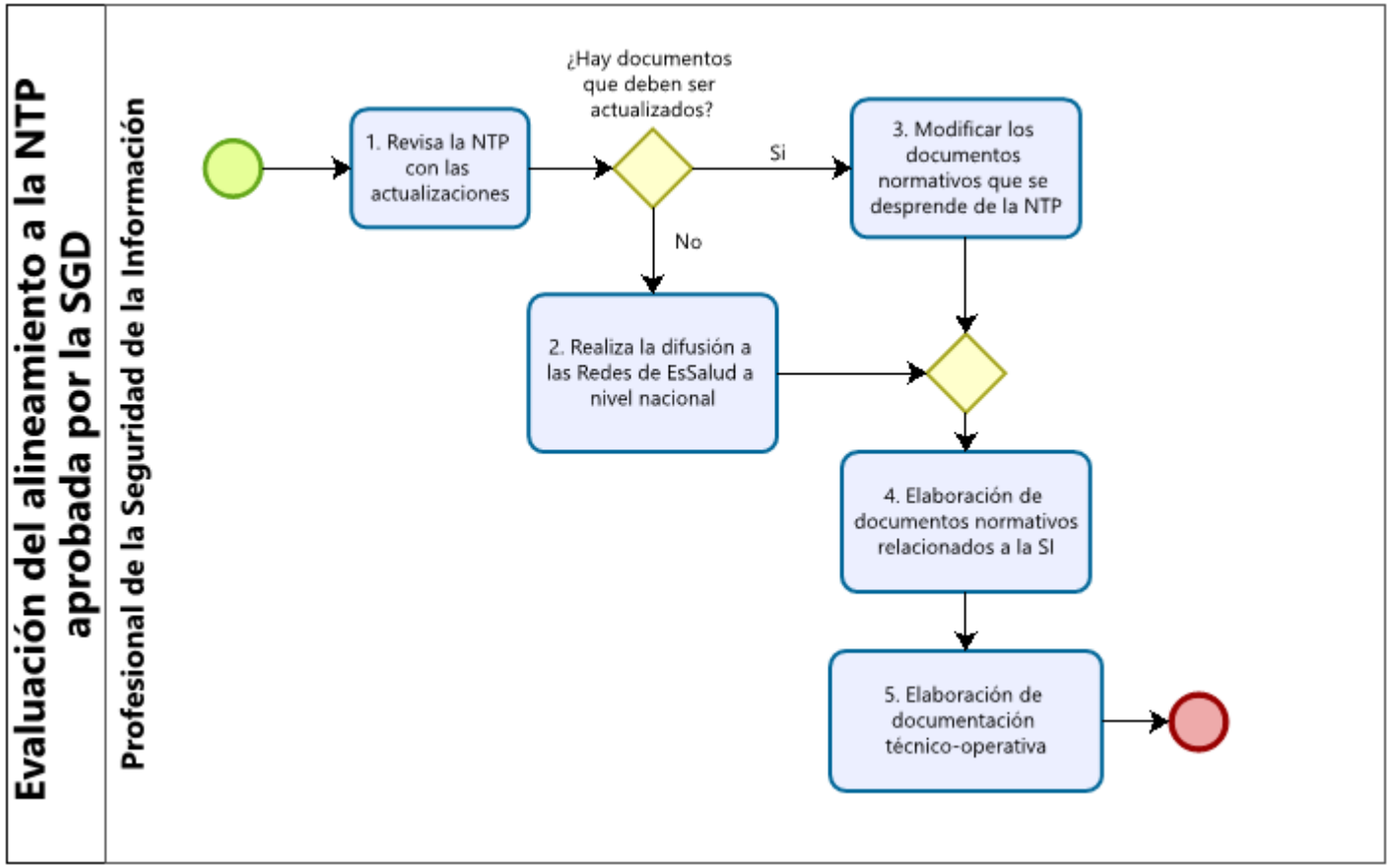
S06.01.01.03 Auditorias del SGSI (Visitas Inopinadas)



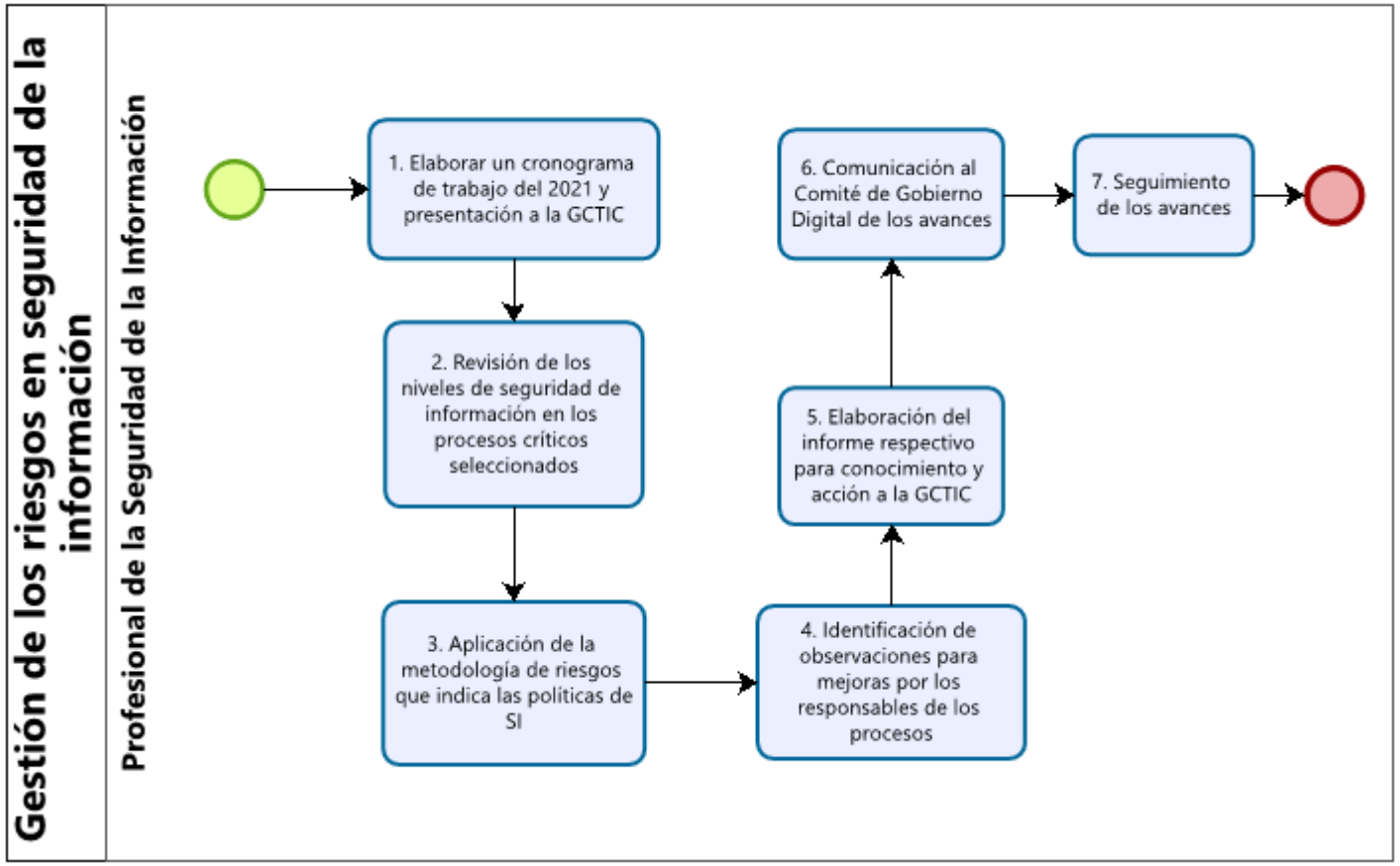
S06.01.01.04 Cumplimiento de Políticas de Seguridad de la Información



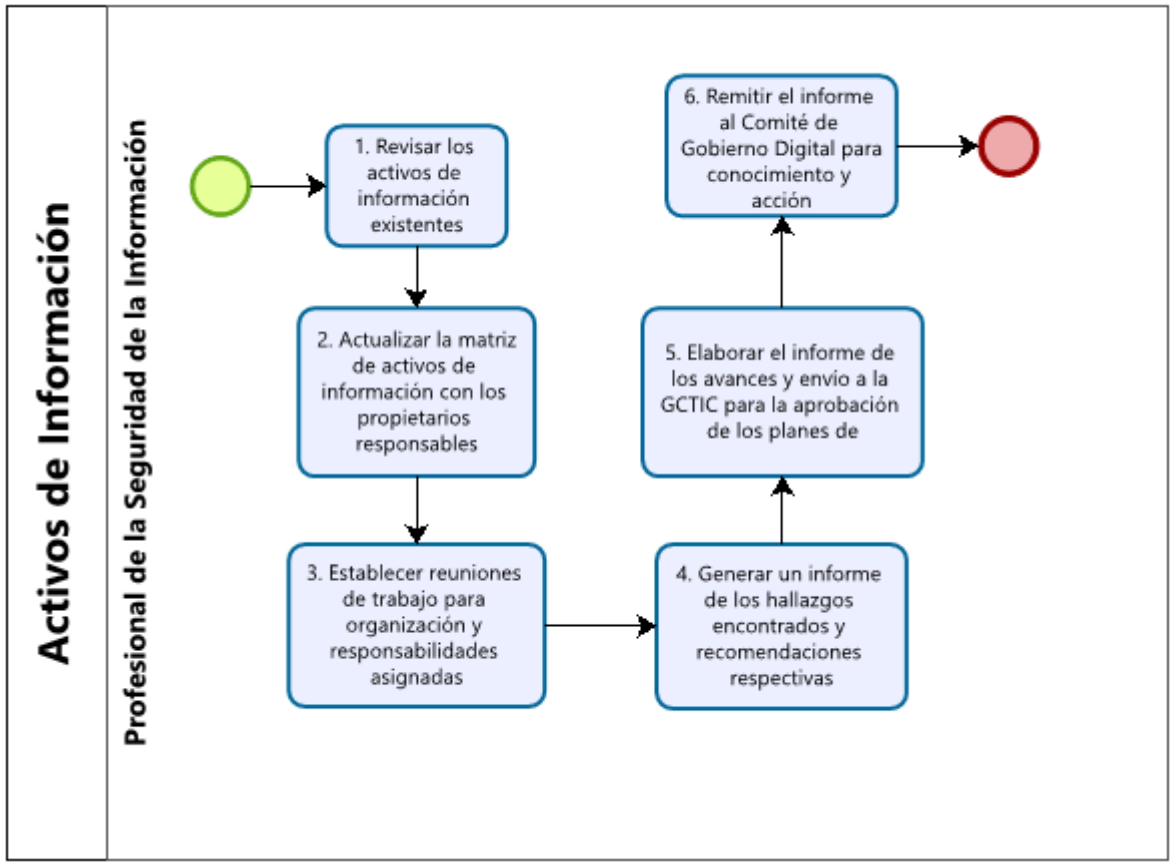
S06.01.01.05 Evaluación del alineamiento a la Norma Técnica Peruana aprobada por la Secretaria de Gobierno Digital



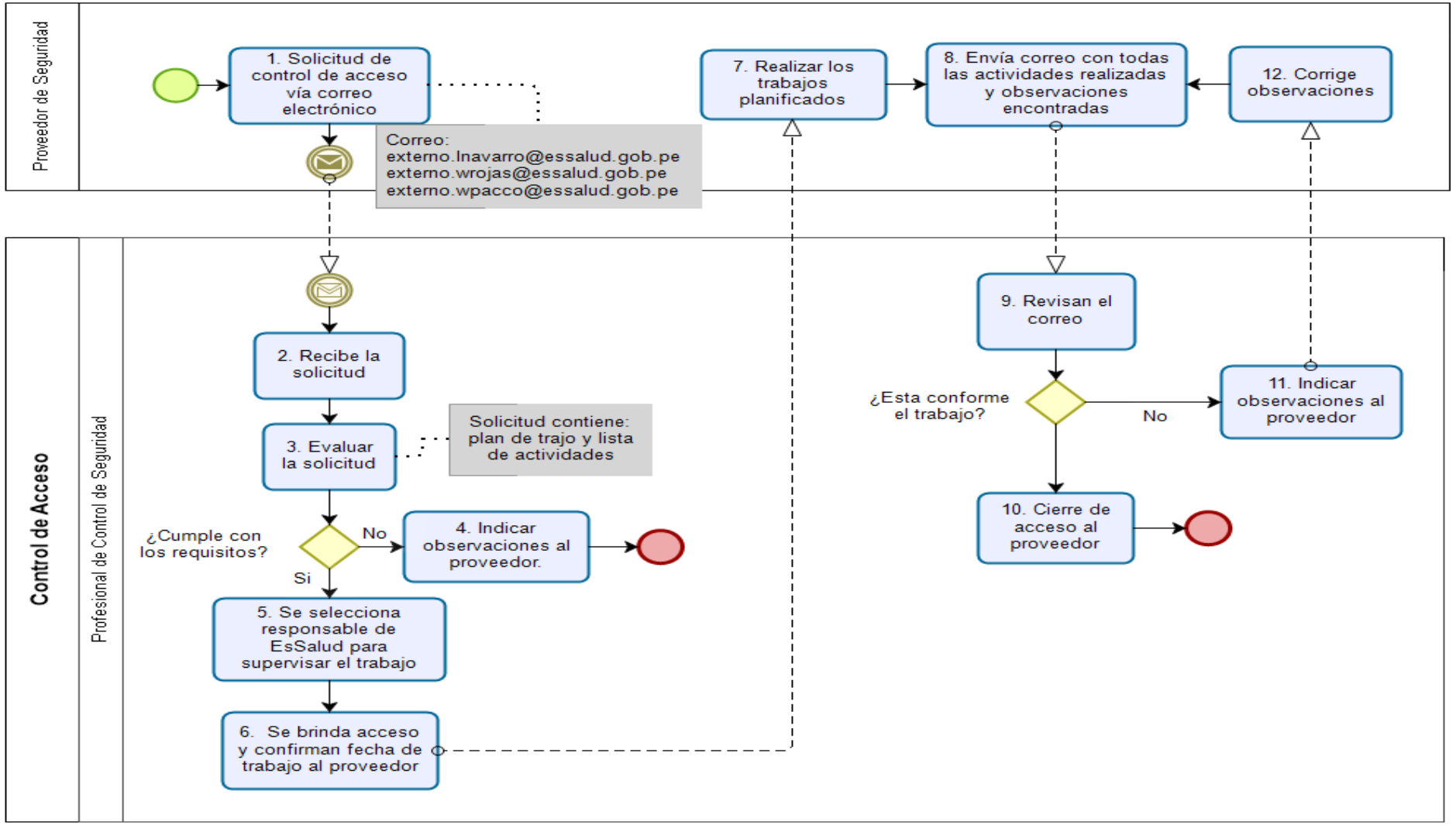
S06.01.01.06 Gestión de los riesgos en Seguridad de la Información (**)



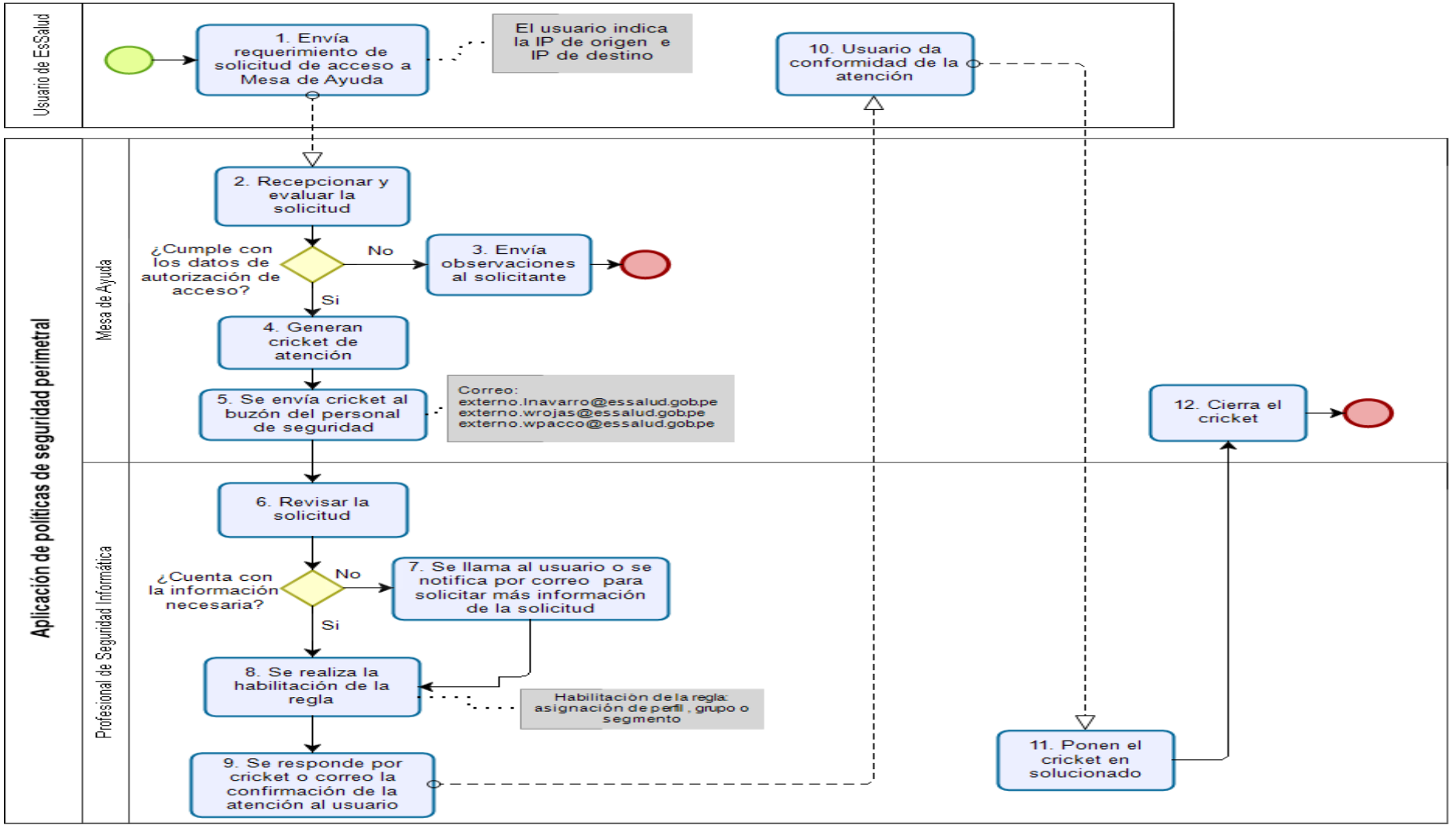
S06.01.01.07 Activos de Información (**)



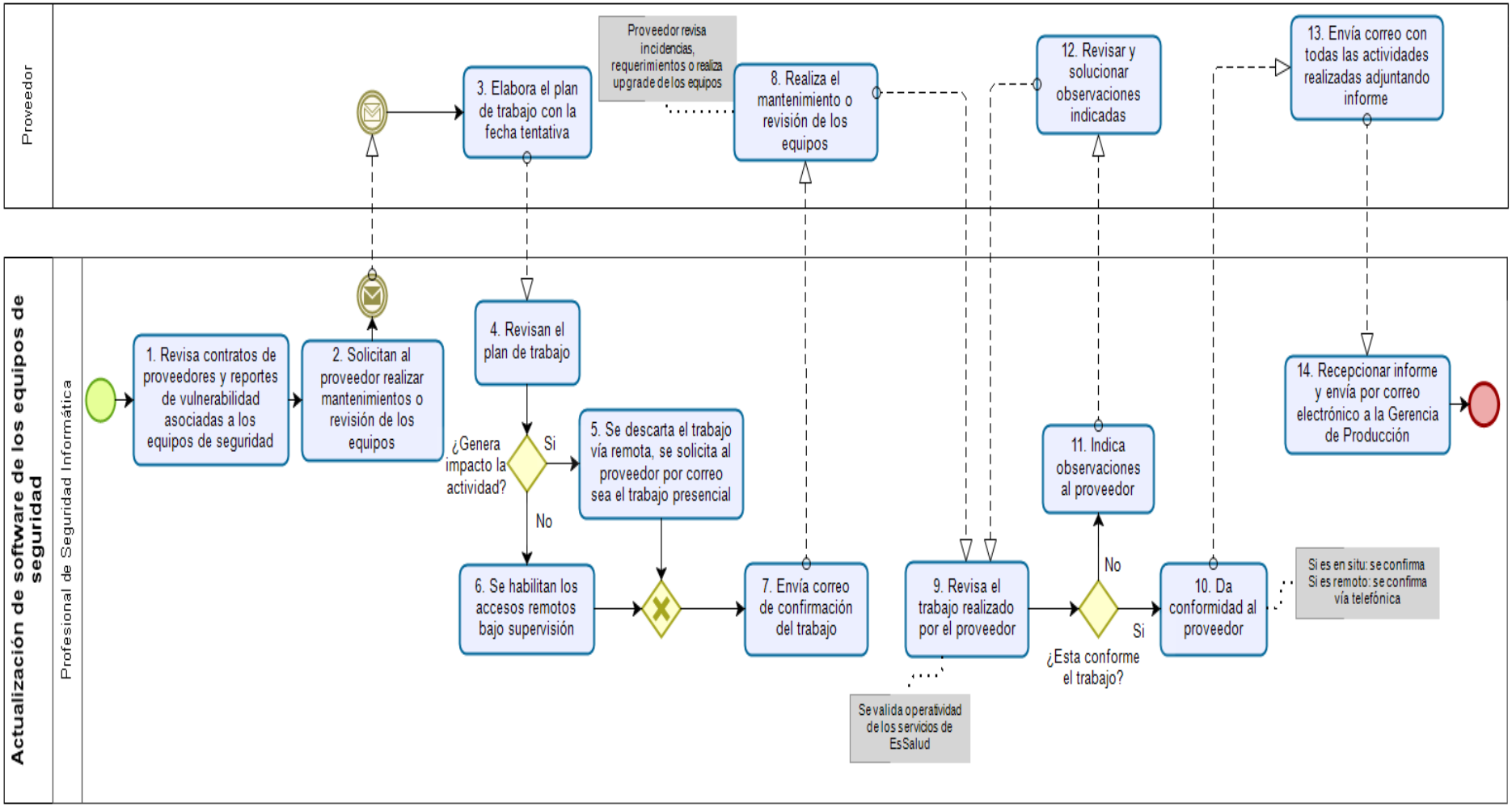
S06.01.02.01.01 Control de Accesos



S06.01.02.01.02 Aplicación de políticas de seguridad perimetral y de la red de datos institucional


Usuario de EsSalud
1. Envía requerimiento de solicitud de acceso a Mesa de Ayuda
El usuario indica la IP de origen e IP de destino
10. Usuario da conformidad de la atención
Aplicación de políticas de seguridad perimetral
Mesa de Ayuda
2. Recepcionar y evaluar la solicitud
¿Cumple con los datos de autorización de acceso?
No
3. Envía observaciones al solicitante
Si
4. Generan cricket de atención
5. Se envía cricket al buzón del personal de seguridad
Correo:
externo.lnavarro@essalud.gobpe
externo.wrojas@essalud.gobpe
externo.wpacco@essalud.gobpe
12. Cierra el cricket
Profesional de Seguridad Informática
6. Revisar la solicitud
¿Cuenta con la información necesaria?
No
7. Se llama al usuario o se notifica por correo para solicitar más información de la solicitud
Si
8. Se realiza la habilitación de la regla
Habilitación de la regla: asignación de perfil , grupo o segmento
9. Se responde por cricket o correo la confirmación de la atención al usuario
11. Ponen el cricket en solucionado

S06.01.02.02.03 Gestión de incidentes



9.4 Ficha de procedimiento

S06.01.01.01: Administración del SGSI (**)

FICHA TÉCNICA DE PROCEDIMIENTO					
Nombre	Administración del SGSI				
Objetivo	Administrar el sistema de la gestión de la seguridad de información de EsSalud.				
Alcance	Diagnóstico y elaboración de políticas alineadas al requerimiento de la Ley de Gobierno Digital. Elaboración del Plan de Trabajo.				
Proveedor	**Entrada**	**Descripción de Actividades**		**Salidas**	**Destinatario de los bienes y servicios**
		Lista de Actividades	**Ejecutor**		
- Presidencia de Consejos de Ministros - Oficina de Control Institucional - Normas ISO internacionales - INACAL	Documentos de SEDGI, OCI, NTP, auditoría externa	1. Revisión de la documentación de las gestiones anteriores de la Oficina de Seguridad Informática 2. Elaborar un diagnóstico por dominio de la NTP/ISO 27001 3. Identificar los controles existentes 4. Alinear con los objetivos estratégicos de la institución y de la GCTIC 5. Elaborar un Informe técnico del diagnóstico 6. Remitir el informe técnico del diagnóstico a la GCTIC 7. Preparar el documento del requerimiento para aprobación de la GCTIC 8. Remitir el Plan de Trabajo a la GCTIC, luego de la aprobación 9. Preparar el documento para aprobación del Comité de Gobierno Digital 10. Elaboración de las políticas de seguridad de información 11. Remitir a la GCTIC y al Comité de Gobierno Digital para aprobación y difusión	Profesional de Seguridad de Información	- Políticas de Seguridad de la Información - Plan de SGSI - Normativa sobre Protección de Datos Personales - Metodología de Riesgos escogida para utilizarla en EsSalud	Usuarios internos y externos que utilizan los Sistemas de EsSalud
Indicadores	(Número total de Informes técnicos del SGSI / (Total de Informes técnicos de la OSI) *100 (Número total de Normas aprobadas / Total de normas difundidas a nivel nacional) *100				
Registros	Inventario de activos, documentos				

*** Al referirnos "Seguridad Informática" es a nivel de proceso, la gestión misma de la materia. De la misma forma, para Seguridad de Información. Ambos procesos registrados en el manual vienen ajustándose por la Oficina de Seguridad Informática de la GCTIC desde Julio del 2021 en base a los requerido en la NTP ISO/IEC 27001:2014.*

S06.01.01.02: Operaciones del SGSI

<table>
<tr><th colspan="6">FICHA TÉCNICA DE PROCEDIMIENTO</th></tr>
<tr><td>Nombre</td><td colspan="5">Operaciones del SGSI</td></tr>
<tr><td>Objetivo</td><td colspan="5">Garantizar la efectividad de los controles de seguridad de información en ESSALUD, a través de actividades analíticas, de diagnóstico, de verificación, de pruebas y de evaluación que permitan alinearse a los requerimientos de la PCM.</td></tr>
<tr><td>Alcance</td><td colspan="5">Primera Fase: Elaboración de informes técnicos de seguridad de información por dominios requeridos en la ISO NTP 27001.</td></tr>
<tr><td rowspan="2">Proveedor</td><td rowspan="2">Entrada</td><td colspan="2">Descripción de Actividades</td><td rowspan="2">Salidas</td><td rowspan="2">Destinatario de los bienes y servicios</td></tr>
<tr><td>Lista de Actividades</td><td>Ejecutor</td></tr>
<tr><td rowspan="4">- Oficina de Seguridad Informática
- Profesional de Seguridad de la Información</td><td rowspan="4">Documentos normativos aprobados</td><td>1. Elaboración de la metodología de trabajo, modelo PDCA (Plan, Do, Check, Act)</td><td rowspan="4">Profesional de Seguridad de Información</td><td rowspan="4">- Informe de incidentes de SI
- Informe de vulnerabilidades
- informe de evaluación de herramientas de SI
- Informe de evaluación de los servicios de las herramientas SI
- Informe de impacto comercial
- Informe de Diseño y Arquitectura de sistemas y/o aplicaciones
- Gestión de Riesgos de Seguridad de la Información</td><td rowspan="4">- Gerencia Central de Tecnologías de Información y Comunicaciones - Redes asistenciales a nivel nacional</td></tr>
<tr><td>2. Aplicación del modelo PDCA a un proceso de la GCTIC</td></tr>
<tr><td>3. Elaboración del informe técnico usando la metodología de trabajo para todos los dominios de la revisión basadas en la NTP ISO 27001, a la GCTIC para su aprobación</td></tr>
<tr><td>4. Remitir informe técnico al Comité de Gobierno Digital</td></tr>
<tr><td>Indicadores</td><td colspan="5">(Número de informes de metodología PDCA aplicada del SGSI / Total de Informes Técnicos de la OSI) *100</td></tr>
<tr><td>Registros</td><td colspan="5">Inventario de activos, documentos</td></tr>
</table>

S06.01.01.03: Auditorias del SGSI (Visitas Inopinadas)

<table>
<tr><th colspan="6">FICHA TÉCNICA DE PROCEDIMIENTO</th></tr>
<tr><td>Nombre</td><td colspan="5">Auditorias del SGSI (Visitas Inopinadas)</td></tr>
<tr><td>Objetivo</td><td colspan="5">Efectuar visitas inopinadas y capacitaciones al personal que permitan mejorar los controles de seguridad de información y difundir la cultura de la seguridad de información en Essalud</td></tr>
<tr><td>Alcance</td><td colspan="5">En procesos críticos y vinculados a la red de atención donde se encuentra los jefes de soporte informático</td></tr>
<tr><td rowspan="2">Proveedor</td><td rowspan="2">Entrada</td><td colspan="2">Descripción de Actividades</td><td rowspan="2">Salidas</td><td rowspan="2">Destinatario de los bienes y servicios</td></tr>
<tr><td>Lista de Actividades</td><td>Ejecutor</td></tr>
<tr><td rowspan="5">- Oficina de Seguridad Informática
- Profesional de la Seguridad de la Información</td><td rowspan="5">Listado de visitas a la Redes Asistenciales de EsSalud</td><td>1. Elaborar el informe técnico de las visitas inopinadas</td><td rowspan="5">Profesional de la Seguridad de la Información</td><td rowspan="5">- Programación de planes de auditoria y supervisión
- Informe técnico de visita
- Rendición de cuentas</td><td rowspan="5">- Gerente de Red, Personal de la Red Asistencial y Administrativo</td></tr>
<tr><td>2. Elaborar el plan de capacitación al personal</td></tr>
<tr><td>3. Preparar material para la capacitación</td></tr>
<tr><td>4. Informar a la GCTIC y al Comité de Gobierno Digital las capacitaciones realizadas y los hallazgos encontrados para conocimiento y acción</td></tr>
<tr><td>5. Informar los hallazgos de seguridad de información encontrados en la red a la GCTIC y al Comité de Gobierno Digital para conocimiento y acción de mejora</td></tr>
<tr><td>Indicadores</td><td colspan="5">(Número de visitas inopinadas planificadas / Número de visitas inopinadas realizadas) *100</td></tr>
<tr><td>Registros</td><td colspan="5">Actas de Visitas Inopinadas</td></tr>
</table>

S06.01.01.04: Cumplimiento de Políticas de Seguridad de la Información

<table>
<tr><th colspan="6">FICHA TÉCNICA DE PROCEDIMIENTO</th></tr>
<tr><td>Nombre</td><td colspan="5">Cumplimiento de Políticas de Seguridad de la Información</td></tr>
<tr><td>Objetivo</td><td colspan="5">Evaluación del cumplimiento de las políticas de seguridad de información</td></tr>
<tr><td>Alcance</td><td colspan="5">Se tomarán muestras (de procesos críticos, de cantidad de elementos revisados, entre otros) por los dominios de control de accesos, incidentes de seguridad de información, seguridad, arquitecturas y diseños, impacto comercial y productos de seguridad.</td></tr>
<tr><td rowspan="2">Proveedor</td><td rowspan="2">Entrada</td><td colspan="2">Descripción de Actividades</td><td rowspan="2">Salidas</td><td rowspan="2">Destinatario de los bienes y servicios</td></tr>
<tr><td>Lista de Actividades</td><td>Ejecutor</td></tr>
<tr><td rowspan="4">Oficina de Seguridad Informática</td><td rowspan="4">- Documentos referidos a la seguridad de información
- Solicitud de consulta sobre procedimientos de seguridad de información</td><td>1. Revisión del checklist de controles de seguridad de información requeridos por dominio de la ISO 27001.</td><td rowspan="4">Profesional de la Seguridad de la Información</td><td rowspan="4">- Planes de Acción de Auditoria de la OSI
- Matriz de Activos
- Plan de Acción de la Ley de Protección de Datos</td><td rowspan="4">- Comité de Gobierno Digital
- Gerencia Central de Tecnologías de Información y Comunicaciones - Jefe de OSI a Nivel Nacional
- Profesionales de Seguridad de la Información</td></tr>
<tr><td>2. Documentación de las evidencias de la revisión</td></tr>
<tr><td>3. Elaboración del informe técnico de cumplimiento</td></tr>
<tr><td>4. Remitir los requerimientos provenientes de las observaciones del informe técnico, al Comité de Gobierno Digital</td></tr>
<tr><td>Indicadores</td><td colspan="5">(Número total de Normas elaboradas / Total de normas aprobadas y difundidas a nivel nacional) *100</td></tr>
<tr><td>Registros</td><td colspan="5">Listado de Indicadores</td></tr>
</table>

S06.01.01.05: Evaluación del alineamiento a la Norma Técnica Peruana aprobada por la Secretaria de Gobierno Digital

<table>
<tr><th colspan="6">FICHA TÉCNICA DE PROCEDIMIENTO</th></tr>
<tr><td>Nombre</td><td colspan="5">Evaluación del alineamiento a la Norma Técnicas Peruana aprobada por la Secretaria de Gobierno Digital</td></tr>
<tr><td>Objetivo</td><td colspan="5">Contar con normas actualizadas y cumplir con la Legislación Aplicable</td></tr>
<tr><td>Alcance</td><td colspan="5">Inicio: Realizar requerimiento de Adquisición de normas vigentes
Fin: Aprobación de Normatividad</td></tr>
<tr><td rowspan="2">Proveedor</td><td rowspan="2">Entrada</td><td colspan="2">Descripción de Actividades</td><td rowspan="2">Salidas</td><td rowspan="2">Destinatario de los bienes y servicios</td></tr>
<tr><td>Lista de Actividades</td><td>Ejecutor</td></tr>
<tr><td rowspan="7">- Presidencia de Consejos de Ministros
- Oficina de Seguridad Informática</td><td rowspan="7">Norma Técnica Peruana</td><td>1. Revisa la NTP con las actualizaciones</td><td rowspan="7">Profesional de la Seguridad de la Información</td><td rowspan="7">Documentos normativos modificados</td><td rowspan="7">Todas las áreas de EsSalud, Postores, Proveedores</td></tr>
<tr><td>¿Hay documentos que deben ser actualizados?

No: ir a actividad 2
Si: ir a actividad 3</td></tr>
<tr><td>2. Realiza la difusión a las Redes de EsSalud a nivel nacional</td></tr>
<tr><td>3. Modificar los documentos normativos que se desprende de la NTP</td></tr>
<tr><td>4. Elaboración de documentos normativos relacionados a la SI</td></tr>
<tr><td>5. Elaboración de documentación técnico-operativa para la implementación y operación para las plataformas tecnologías en seguridad informática</td></tr>
<tr><td>Indicadores</td><td colspan="5">(Número de Normas revisadas / Total de Normas actualizadas) * 100</td></tr>
<tr><td>Registros</td><td colspan="5">Listado de Normas</td></tr>
</table>

S06.01.01.06: Gestión de los riesgos en Seguridad de la Información (**)

<table>
<tr><th colspan="6">FICHA TÉCNICA DE PROCEDIMIENTO</th></tr>
<tr><td>Nombre</td><td colspan="5">Gestión de los riesgos en seguridad de la información</td></tr>
<tr><td>Objetivo</td><td colspan="5">Evaluación de la matriz de gestión de riesgos de seguridad de información de EsSalud</td></tr>
<tr><td>Alcance</td><td colspan="5">Primera Fase: procesos críticos vinculados al sistema ESSI</td></tr>
<tr><td rowspan="2">Proveedor</td><td rowspan="2">Entrada</td><td colspan="2">Descripción de Actividades</td><td rowspan="2">Salidas</td><td rowspan="2">Destinatario de los bienes y servicios</td></tr>
<tr><td>Lista de Actividades</td><td>Ejecutor</td></tr>
<tr><td rowspan="8">- Profesional de Seguridad de la Información
- Usuario de EsSalud</td><td rowspan="8">- Herramientas de seguridad
- Identificación del riesgo de seguridad
- Documentos de tratamiento de eventos relacionados al marco de la seguridad y privacidad</td><td>1. Elaborar un cronograma de trabajo del 2021 y presentación a la GCTIC</td><td rowspan="8">Profesional de la Seguridad de la Información</td><td rowspan="8">Documentos de control de mitigación de riesgo de seguridad</td><td rowspan="8">- Oficina de Seguridad Informática EsSalud
- Gerencia de Producción
- Gerencia Central de Tecnologías de Información y Comunicaciones</td></tr>
<tr><td>2. Revisión de los niveles de seguridad de información en los procesos críticos seleccionados</td></tr>
<tr><td>3. Aplicación de la metodología de riesgos que indica las políticas de seguridad de información para los procesos críticos seleccionados</td></tr>
<tr><td>4. Identificación de observaciones para mejoras por los responsables de los procesos (propietarios)</td></tr>
<tr><td>5. Elaboración del informe respectivo para conocimiento y acción a la GCTIC</td></tr>
<tr><td>6. Comunicación al Comité de Gobierno Digital de los avances</td></tr>
<tr><td>7. Seguimiento de los avances</td></tr>
<tr><td>Indicadores</td><td colspan="5">(Número de Informes dirigidos a la GCTIC / Número de informes presentados a la GCTIC) *</td></tr>
<tr><td>Registros</td><td colspan="5">Plan de respuesta a incidentes de Seguridad de la Información / Metodología de Riesgos escogida para el año en curso</td></tr>
</table>

S06.01.01.07: Activos de Información (**)

<table>
<tr><th colspan="6">FICHA TÉCNICA DE PROCEDIMIENTO</th></tr>
<tr><td>Nombre</td><td colspan="5">Activos de Información</td></tr>
<tr><td>Objetivo</td><td colspan="5">Evaluación de la matriz de activos de información de EsSalud</td></tr>
<tr><td>Alcance</td><td colspan="5">Primera Fase: GCTIC</td></tr>
<tr><td rowspan="2">Proveedor</td><td rowspan="2">Entrada</td><td colspan="2">Descripción de Actividades</td><td rowspan="2">Salidas</td><td rowspan="2">Destinatario de los bienes y servicios</td></tr>
<tr><td>Lista de Actividades</td><td>Ejecutor</td></tr>
<tr><td rowspan="6">- Oficina de Seguridad Informática EsSalud
- Usuario de EsSalud a Nivel Nacional</td><td rowspan="6">- Documentos de clasificación de activos
- Documento de criticidad y aplicabilidad de activos de información críticos</td><td>1. Revisar los activos de información existentes</td><td rowspan="6">Profesional de la Seguridad de la Información</td><td rowspan="6">Documentos de control de Clasificación y criticidad de activos de información</td><td rowspan="6">- Gerencia Central de Tecnologías de Información y Comunicaciones
- Usuarios internos y externos que utilizan los activos de información de EsSalud</td></tr>
<tr><td>2. Actualizar la matriz de activos de información con los propietarios responsables</td></tr>
<tr><td>3. Establecer reuniones de trabajo para organización y responsabilidades asignadas</td></tr>
<tr><td>4. Generar un informe de los hallazgos encontrados y recomendaciones respectivas</td></tr>
<tr><td>5. Elaborar el informe de los avances y envío a la GCTIC para la aprobación de los planes de acción</td></tr>
<tr><td>6. Remitir el informe al Comité de Gobierno Digital para conocimiento y acción</td></tr>
<tr><td>Indicadores</td><td colspan="5">(Número de activos de información clasificados / Total de activos de información clasificados) *100</td></tr>
<tr><td>Registros</td><td colspan="5">Correos electrónicos, matriz de clasificación de activos</td></tr>
</table>

S06.01.02.01.01: Control de Accesos (**)

<table>
<tr><th colspan="6">FICHA TÉCNICA DE PROCEDIMIENTO</th></tr>
<tr><td>Nombre</td><td colspan="5">Control de Acceso</td></tr>
<tr><td>Objetivo</td><td colspan="5">Realizar el control y seguimiento a las actividades realizadas por parte del proveedor de servicios de operación y validar el cumplimiento de estas.</td></tr>
<tr><td>Alcance</td><td colspan="5">Gerencia Central de Tecnologías de Información y Comunicaciones</td></tr>
<tr><td rowspan="2">Proveedor</td><td rowspan="2">Entrada</td><td colspan="2">Descripción de Actividades</td><td rowspan="2">Salidas</td><td rowspan="2">Destinatario de los bienes y servicios</td></tr>
<tr><td>Lista de Actividades</td><td>Ejecutor</td></tr>
<tr><td rowspan="13">- Normas ISO internacionales / INACAL
- PCM, Grupos de trabajo (Seguridad de Información), Foros Nacionales e Internacionales, Proveedores de SI
- Unidades orgánicas de EsSalud</td><td rowspan="13">- Informes del área responsable de atenciones críticas de acceso a operación
- Informes consolidado del área responsable de los servicios de operación</td><td>Solicitud de control de acceso vía correo electrónico</td><td>Proveedor de operación de herramientas de Seguridad</td><td rowspan="13">- Formulario de cambio por cada herramienta de seguridad.
- Formulario de acceso a base de datos.
- Formulario de acceso a servicios.
- Formulario de acceso para entidades externas.
- Formulario de solicitud de cuentas VPN SSL e IPsec
- Formato de Aceptación de Riesgos</td><td rowspan="13">- Unidades orgánicas de EsSalud
- Redes asistenciales
- Redes prestacionales
- Proveedores
- Asegurados</td></tr>
<tr><td>Recibe la solicitud</td><td rowspan="4">- OSI
- Profesional de la Seguridad de la Información</td></tr>
<tr><td>Evaluar la solicitud</td></tr>
<tr><td>Indicar observaciones al área ejecutora</td></tr>
<tr><td>Se selecciona responsable del área ejecutora de EsSalud para verificar el trabajo</td></tr>
<tr><td>Se brinda acceso y confirman fecha de trabajo al proveedor</td><td>Profesional de Control del área ejecutora</td></tr>
<tr><td>Realizar los trabajos planificados</td><td rowspan="2">Proveedor de operación de herramientas de Seguridad</td></tr>
<tr><td>Envía correo con todas las actividades realizadas</td></tr>
<tr><td>Revisar el correo</td><td rowspan="2">Profesional de Control del área ejecutora</td></tr>
<tr><td>Cierre de atención del acceso solicitado</td></tr>
<tr><td>Indicar observaciones al proveedor</td><td>- OSI
- Profesional de la Seguridad de la Información</td></tr>
<tr><td>Corrige observaciones</td><td>Proveedor de operación de herramientas de Seguridad</td></tr>
<tr><td>Indicadores</td><td colspan="5">(Cantidad de accesos solicitados / Cantidad de accesos brindados por el proveedor) *100</td></tr>
<tr><td>Registros</td><td colspan="5">Solicitud de acceso, Consolidados de formularios atendidos, Cronograma de trabajo, Plan de actividades, Registro de altas y bajas de accesos</td></tr>
</table>

S06.01.02.01.02: Aplicación de políticas de seguridad perimetral y de la red de datos institucional

<table>
<tr><th colspan="6">FICHA TÉCNICA DE PROCEDIMIENTO</th></tr>
<tr><td>Nombre</td><td colspan="5">Aplicación de políticas de seguridad perimetral y de la red de datos institucional</td></tr>
<tr><td>Objetivo</td><td colspan="5">Ejecutar las políticas y configuraciones de la seguridad perimetral y de la red de datos institucional, aplicando los controles y las buenas prácticas en Seguridad de la Información</td></tr>
<tr><td>Alcance</td><td colspan="5">Gerencia Central de Tecnologías de Información y Comunicaciones</td></tr>
<tr><td rowspan="2">Proveedor</td><td rowspan="2">Entrada</td><td colspan="2">Descripción de Actividades</td><td rowspan="2">Salidas</td><td rowspan="2">Destinatario de los bienes y servicios</td></tr>
<tr><td>Lista de Actividades</td><td>Ejecutor</td></tr>
<tr><td rowspan="15">- Normas ISO internacionales / INACAL
- PCM, Grupos de trabajo (Seguridad de Información), Foros Nacionales e Internacionales, Proveedores de SI
- Unidades orgánicas de EsSalud</td><td rowspan="15">- Informes del área responsable de los servicios de operación por cumplimiento de controles</td><td>Solicitud de controles para aplicación</td><td>Proveedor de operación de herramientas de Seguridad</td><td rowspan="15">- Informe de controles normativos aplicados alineados a las NTP 27001:2014
- Informe de cumplimiento de controles aplicados a la operación de herramientas de seguridad.
- Formato de Aceptación de Riesgos</td><td rowspan="15">- Unidades orgánicas de EsSalud
- Redes asistenciales
- Redes prestacionales
- Proveedores
- Asegurados</td></tr>
<tr><td>Recibe la solicitud</td><td>Profesional de Control del área ejecutora</td></tr>
<tr><td>Envía solicitud a la OSI</td><td rowspan="4">- OSI
- Profesional de la Seguridad de la Información</td></tr>
<tr><td>Evaluar la solicitud</td></tr>
<tr><td>Indicar observaciones al área ejecutora</td></tr>
<tr><td>Se selecciona responsable del área ejecutora de EsSalud para verificar el cumplimiento</td></tr>
<tr><td>Se hace de conocimiento del proveedor para aplicación de controles</td><td>Profesional de Control del área ejecutora</td></tr>
<tr><td>Realizar los trabajos planificados de aplicación de controles</td><td rowspan="2">Proveedor de operación de herramientas de Seguridad</td></tr>
<tr><td>Envía correo con todas las actividades realizadas</td></tr>
<tr><td>Revisar el correo</td><td rowspan="2">Profesional de Control del área ejecutora</td></tr>
<tr><td>Cierre de atención de controles aplicados a los incidentes</td></tr>
<tr><td>Indicar observaciones al proveedor</td><td rowspan="2">- OSI
- Profesional de la Seguridad de la Información</td></tr>
<tr><td>Corrige observaciones</td></tr>
<tr><td>Indicadores</td><td colspan="5">(Cantidad de controles solicitados para ser aplicados / Cantidad de controles aplicados) *100</td></tr>
<tr><td>Registros</td><td colspan="5">Normatividad aprobada para aplicación, Informe de controles normativos aplicados, Términos de referencia alineadas a la NTP 27001, Especificaciones técnicas alineadas a la NTP 27001, Informe y planes de realización de actividades</td></tr>
</table>

S06.01.02.02.03: Gestión de incidentes (**)

<table>
<tr><th colspan="6">FICHA TÉCNICA DE PROCEDIMIENTO</th></tr>
<tr><td>Nombre</td><td colspan="5">Gestión de incidentes</td></tr>
<tr><td>Objetivo</td><td colspan="5">Garantizar la continuidad operativa a partir de la óptima gestión de incidentes, mitigando los riesgos y brechas de seguridad a partir de la aplicación de controles y conocimiento</td></tr>
<tr><td>Alcance</td><td colspan="5">Gerencia Central de Tecnologías de Información y Comunicaciones</td></tr>
<tr><td rowspan="2">Proveedor</td><td rowspan="2">Entrada</td><td colspan="2">Descripción de Actividades</td><td rowspan="2">Salidas</td><td rowspan="2">Destinatario de los bienes y servicios</td></tr>
<tr><td>Lista de Actividades</td><td>Ejecutor</td></tr>
<tr><td rowspan="15">- Normas ISO internacionales / INACAL
- PCM, Grupos de trabajo (Seguridad de Información), Foros Nacionales e Internacionales, Proveedores de SI
- Unidades orgánicas de EsSalud</td><td rowspan="15">- Planes de implementación y migración
- Contrato de proveedores
- Reportes de vulnerabilidad</td><td>Solicitud de controles para aplicación</td><td>Proveedor de operación de herramientas de Seguridad</td><td rowspan="15">- Plan de actividades
- Plan de Roll Back
- Plan de Backup
- Evaluación de impacto potencial en los servicios
- Formato de Aceptación de Riesgos</td><td rowspan="15">- Unidades orgánicas de EsSalud
- Redes Asistenciales
- Redes Prestacionales
- Proveedores
- Asegurados</td></tr>
<tr><td>Recibe comunicación de incidentes</td><td>Profesional de Control del área ejecutora</td></tr>
<tr><td>Envía comunicación a la OSI</td><td rowspan="4">- OSI
- Profesional de la Seguridad de la Información</td></tr>
<tr><td>Evaluar incidentes

Implicancia en la continuidad operativa</td></tr>
<tr><td>Indicar observaciones al área ejecutora</td></tr>
<tr><td>Se selecciona responsable del área ejecutora de EsSalud para tareas de mitigación</td></tr>
<tr><td>Se hace de conocimiento del proveedor para aplicación de controles</td><td>Profesional de Control del área ejecutora</td></tr>
<tr><td>Realizar los trabajos planificados de aplicación de controles para mitigación de incidentes</td><td rowspan="3">Proveedor de operación de herramientas de Seguridad</td></tr>
<tr><td>Envía correo con todas las actividades realizadas

Resolución de incidentes</td></tr>
<tr><td>Revisar el correo</td><td rowspan="3">Profesional de Control del área ejecutora</td></tr>
<tr><td>Cierre de atención de controles aplicados a partir de las políticas</td></tr>
<tr><td>Indicar observaciones al proveedor</td><td rowspan="3">- OSI
- Profesional de la Seguridad de la Información</td></tr>
<tr><td>Corrige observaciones</td></tr>
<tr><td>Indicadores</td><td colspan="5">(Cantidad de incidentes reportados / Cantidad de incidentes resueltos) *100</td></tr>
<tr><td>Registros</td><td colspan="5">Informe de controles normativos aplicados
Términos de referencia alineadas a la NTP 27001, Especificaciones técnicas alineadas a la NTP 27001, Plan de actividades, Plan de Roll Back, Plan de Backup, Listado de actividades realizadas, Informe y planes de realización de actividades</td></tr>
</table>

9.5 Ficha de indicadores

S06.01.01.01: Administración del SGSI (**)

FICHA INDICADORES	
Nombre del Proceso	Administración del SGSI
Nombre Indicador	Porcentaje de informes técnicos del SGSI, Normas aprobadas
Descripción del Indicador	Medir el porcentaje de Normas aprobadas
Objetivo del Indicador	Administrar el sistema de la gestión de la seguridad de información de EsSalud
Forma de Cálculo	(Número total de Informes técnicos del SGSI / (Total de Informes técnicos de la OSI) *100 (Número total de Normas elaboradas / Total de normas aprobadas y difundidas a nivel nacional) *100
Fuentes de Información	Inventario de activos, documentos
Periodicidad de Medición	Mensual
Responsable de Medición	Oficina de Seguridad Informática
Meta	100%

S06.01.01.02: Operaciones del SGSI

FICHA INDICADORES	
Nombre del Proceso	Operaciones del SGSI
Nombre Indicador	Porcentaje de informes de metodología PDCA
Descripción del Indicador	Medir el porcentaje de informes de la metodología PDCA a partir de los informes Técnicos emitidos por la OSI
Objetivo del Indicador	Evidenciar la aplicación de controles a partir de los informes de metodología PDCA aplicada del SGSI emitidos por la OSI
Forma de Cálculo	(Número de informes de metodología PDCA aplicada del SGSI / Total de Informes Técnicos de la OSI) *100
Fuentes de Información	Inventario de activos, documentos
Periodicidad de Medición	Mensual
Responsable de Medición	Oficina de Seguridad Informática
Meta	100%

S06.01.01.03: Auditorias del SGSI (Visitas Inopinadas)

FICHA INDICADORES	
Nombre del Proceso	Auditorias del SGSI (Visitas Inopinadas)
Nombre Indicador	Porcentaje de visitas inopinadas
Descripción del Indicador	Medir el porcentaje de visitas inopinadas realizadas
Objetivo del Indicador	Efectuar visitas inopinadas al personal que permitan mejorar los controles de seguridad de información
Forma de Cálculo	(Número de visitas inopinadas planificadas / Número de visitas inopinadas realizadas) *100
Fuentes de Información	Actas de Visitas Inopinadas
Periodicidad de Medición	Mensual
Responsable de Medición	Oficina de Seguridad Informática
Meta	100%

S06.01.01.04: Cumplimiento de Políticas de Seguridad de la Información

FICHA INDICADORES	
Nombre del Proceso	Cumplimiento de Políticas de Seguridad de la Información
Nombre Indicador	Porcentaje de normas elaboradas
Descripción del Indicador	Medir el porcentaje de normas elaboradas, aprobadas y difundidas
Objetivo del Indicador	Evaluar el cumplimiento de las políticas de seguridad de la información aprobadas a nivel nacional
Forma de Cálculo	(Número total de Normas elaboradas / Total de normas aprobadas y difundidas a nivel nacional) *100
Fuentes de Información	Resoluciones, documentos, informes de cumplimiento
Periodicidad de Medición	Mensual
Responsable de Medición	Oficina de Seguridad Informática
Meta	100%

S06.01.01.05: Evaluación del alineamiento a la Norma Técnica Peruana aprobada por la secretaria de Gobierno Digital

FICHA INDICADORES	
Nombre del Proceso	Evaluación del alineamiento a la Norma Técnicas Peruana aprobada por la Secretaria de Gobierno Digital
Nombre Indicador	Porcentaje de Normas revisadas
Descripción del Indicador	Este indicador mide el porcentaje de normas revisadas por la Oficina de Seguridad Informática
Objetivo del Indicador	Identificar el total de normas actualizadas por la Oficina de Seguridad Informática
Forma de Cálculo	(Número de Normas revisadas / Total de Normas actualizadas) * 100
Fuentes de Información	Listado de Normas
Periodicidad de Medición	Mensual
Responsable de Medición	Oficina de Seguridad Informática
Meta	100%

S06.01.01.06: Gestión de los riesgos en Seguridad de la Información

FICHA INDICADORES	
Nombre del Proceso	Gestión de los riesgos en Seguridad de la Información
Nombre Indicador	Porcentaje de Informes dirigidos a la GCTIC
Descripción del Indicador	Medir el porcentaje de informes presentados a la GCTIC
Objetivo del Indicador	Mitigar los riesgos a partir de las vulnerabilidades identificadas a partir de la gestión eficiente de la matriz de riesgos de seguridad de la información
Forma de Cálculo	(Número de Informes elaborados para la GCTIC / Número de informes presentados a la GCTIC) *100
Fuentes de Información	Plan de respuesta a incidentes de Seguridad de la Información / Metodología de Riesgos escogida para el año en curso
Periodicidad de Medición	Mensual
Responsable de Medición	Oficina de Seguridad Informática
Meta	100%

S06.01.01.07: Activos de Información

FICHA INDICADORES	
Nombre del Proceso	Activos de Información
Nombre Indicador	Porcentaje de activos de información identificados
Descripción del Indicador	Medir el porcentaje de activos de información clasificados
Objetivo del Indicador	Evaluar la matriz de activos de información de EsSalud para una óptima gestión de los mismos
Forma de Cálculo	(Número de activos de información identificados / Total de activos de información clasificados) *100
Fuentes de Información	Correos electrónicos, matriz de clasificación de activos
Periodicidad de Medición	Mensual
Responsable de Medición	Oficina de Seguridad Informática
Meta	100%

S06.01.02.01.01: Control de Accesos

FICHA INDICADORES	
Nombre del Proceso	Control de Accesos
Nombre Indicador	Porcentaje de accesos cerrados
Descripción del Indicador	Medir el porcentaje de accesos brindados por el proveedor
Objetivo del Indicador	Realizar el control de accesos y seguimiento a las actividades realizadas por parte del proveedor de servicios de operación
Forma de Cálculo	(Cantidad de accesos solicitados / Cantidad de accesos brindados por el proveedor) *100
Fuentes de Información	Solicitud de acceso, Consolidados de formularios atendidos, Cronograma de trabajo, Plan de actividades, Registro de altas y bajas de accesos
Periodicidad de Medición	Mensual
Responsable de Medición	Subgerencia de Comunicaciones
Meta	100%

S06.01.02.01.02: Aplicación de políticas de seguridad perimetral y de la red de datos institucional

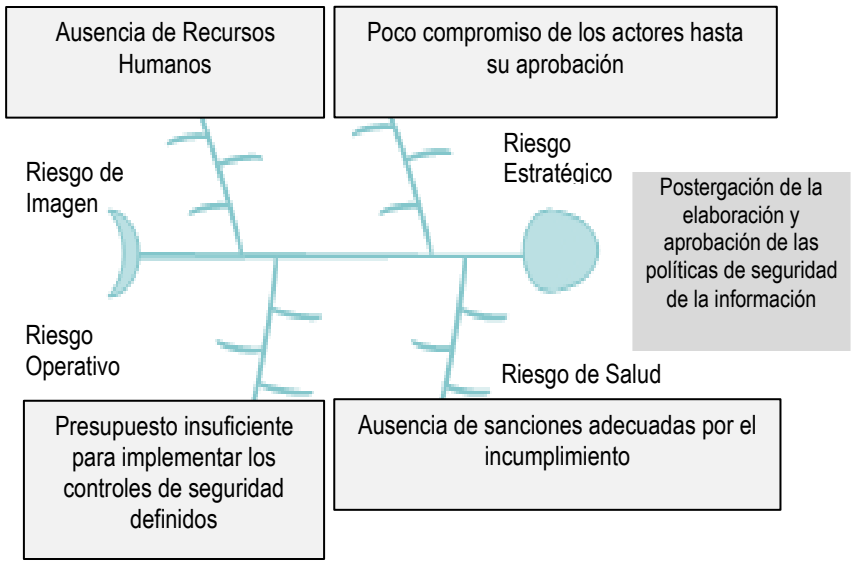
FICHA INDICADORES	
Nombre del Proceso	Aplicación de políticas de seguridad perimetral y de la red de datos institucional
Nombre Indicador	Porcentaje de controles solicitados para ser aplicados
Descripción del Indicador	Medir el porcentaje de controles aplicados
Objetivo del Indicador	Determinar la aplicación de las políticas y configuraciones de la seguridad perimetral y de la red de datos institucional
Forma de Cálculo	(Cantidad de controles solicitados para ser aplicados / Cantidad de controles aplicados) *100
Fuentes de Información	Normatividad aprobada para aplicación, Informe de controles normativos aplicados, Términos de referencia alineadas a la NTP 27001, Especificaciones técnicas alineadas a la NTP 27001, Informe y planes de realización de actividades
Periodicidad de Medición	Mensual
Responsable de Medición	Subgerencia de Comunicaciones
Meta	100%

S06.01.02.02.03: Gestión de Incidentes

FICHA INDICADORES	
Nombre del Proceso	Gestión de Incidentes
Nombre Indicador	Porcentaje de incidentes reportados
Descripción del Indicador	Medir el porcentaje de incidentes resueltos
Objetivo del Indicador	Garantizar la continuidad operativa a partir de la óptima gestión de incidentes
Forma de Cálculo	(Cantidad de incidentes reportados / Cantidad de incidentes resueltos) *100
Fuentes de Información	Informe de controles normativos aplicados Términos de referencia alineadas a la NTP 27001, Especificaciones técnicas alineadas a la NTP 27001, Plan de actividades, Plan de Roll Back, Plan de Backup, Listado de actividades realizadas, Informe y planes de realización de actividades
Periodicidad de Medición	Mensual
Responsable de Medición	Subgerencia de Comunicaciones
Meta	100%

9.6 Ficha de riesgo

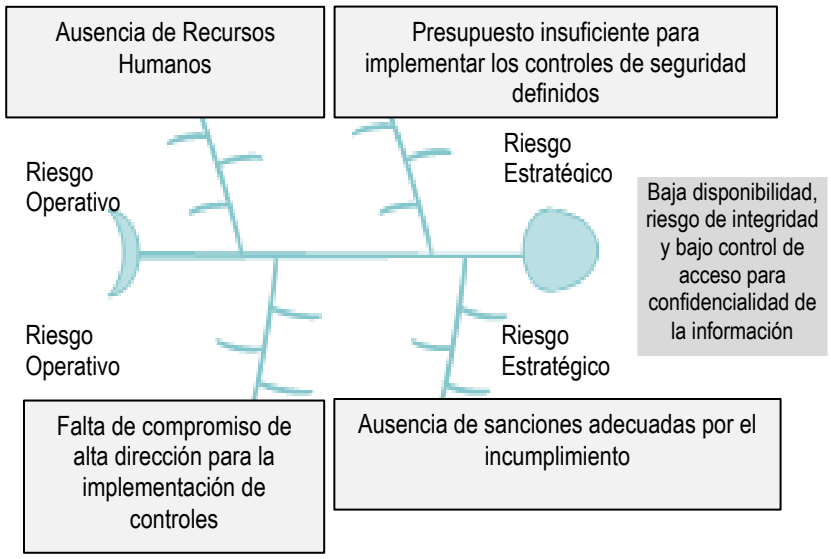
S06.01.01.01: Administración del SGSI

<table>
<tr><th colspan="8">FICHA DE RIESGO</th></tr>
<tr><th colspan="8">FICHA PARA IDENTIFICAR, ANALIZAR Y DAR RESPUESTA AL RIEGOS</th></tr>
<tr><td rowspan="5">1</td><td colspan="2" rowspan="5">NOMBRE DEL PROCESO</td><td>Macroproceso (Nivel 0)</td><td colspan="4">Gestión de Seguridad Integral, Emergencias y Desastres</td></tr>
<tr><td>Proceso (Nivel 1)</td><td colspan="4">Gestión de Seguridad Informática</td></tr>
<tr><td>Subproceso (Nivel 2)</td><td colspan="4">Seguridad de la Información</td></tr>
<tr><td>Procedimiento</td><td colspan="4">Administración del SGSI</td></tr>
<tr><td>Actividad</td><td colspan="4">Diagnóstico y elaboración normativas alineadas a la Ley de Gobierno Digital</td></tr>
<tr><td rowspan="2">2</td><td colspan="2" rowspan="2">OBJETIVO DEL PROCESO</td><td>Descripción</td><td colspan="4">Elaboración de Políticas de Seguridad de la Información alineadas a la NTP 27001</td></tr>
<tr><td>Ubicación (Departamento, Ciudad Distrito)</td><td colspan="4">Lima, Lima, Jesús María</td></tr>
<tr><td>3</td><td colspan="7">IDENTIFICACIÓN DE RIESGOS</td></tr>
<tr><td></td><td>3.1</td><td>TIPO DE RIESGO</td><td colspan="4">Riesgo de Imagen Institucional, Operativo, Estratégico, de Salud</td></tr>
<tr><td></td><td>3.2</td><td>CODIFICACION</td><td colspan="4"></td></tr>
<tr><td></td><td>3.3</td><td>DESCRIPCIÓN DEL RIESGO</td><td colspan="4">Postergación de la elaboración y aprobación de las políticas de seguridad de la información</td></tr>
<tr><td rowspan="4"></td><td rowspan="4">3.4</td><td rowspan="3">CAUSA(S) GENERADORA(S)</td><td colspan="2">Causa N° 1</td><td colspan="2">Ausencia de Recursos Humanos</td></tr>
<tr><td colspan="2">Causa N° 2</td><td colspan="2">Poco compromiso de los actores hasta su aprobación</td></tr>
<tr><td colspan="2">Causa N° 3</td><td colspan="2">Presupuesto insuficiente para implementar los controles de seguridad definidos</td></tr>
<tr><td></td><td colspan="2">Causa N° 4</td><td colspan="2">Ausencia de sanciones adecuadas por el incumplimiento</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2">TECNICA DE DIAGRAMACION</td><td>Diagrama Causa Efecto</td><td colspan="4">Diagrama de Ishikawa</td></tr>
<tr><td>Diagrama de Flujo de Procesos</td><td colspan="4"> 
</td></tr>
<tr><td>4</td><td></td><td colspan="6">VALORACION DEL RIEGO</td></tr>
<tr><td rowspan="8"></td><td rowspan="8">4.1</td><td colspan="3">PROBABILIDAD DE OCURRENCIA</td><td></td><td colspan="2">IMPACTO</td></tr>
<tr><td>Análisis Cualitativo</td><td>Análisis Cuantitativo</td><td></td><td></td><td>Análisis Cualitativo</td><td>Análisis Cuantitativo</td><td></td></tr>
<tr><td>Muy baja</td><td>0.10</td><td></td><td></td><td>Muy bajo</td><td>0.05</td><td></td></tr>
<tr><td>Baja</td><td>0.30</td><td></td><td></td><td>Bajo</td><td>0.10</td><td></td></tr>
<tr><td>Moderada</td><td>0.50</td><td></td><td></td><td>Moderado</td><td>0.20</td><td></td></tr>
<tr><td>Alta</td><td>0.70</td><td></td><td></td><td>Alto</td><td>0.40</td><td></td></tr>
<tr><td>Muy alta</td><td>0.90</td><td>0.90</td><td></td><td>Muy alto</td><td>0.80</td><td></td></tr>
<tr><td colspan="2">Muy Alta</td><td>0.90</td><td></td><td colspan="2">Muy Alto</td><td>0.80</td></tr>
</table>

	4.3	PRIORIZACIÓN DEL RIESGO				
		Puntuación del Riesgo =Probabilidad x Impacto	0.72	Prioridad del Riesgo	Muy Alta Prioridad	
5	RESPUESTA A LOS RIESGOS					
	5.1	ESTRATEGIA	Mitigar Riesgo	X	Evitar Riesgo	
			Aceptar Riesgo		Transferir Riesgo	
	5.2	RIESGO ASIGNADO A (Solo después de haber marcado Transferir el Riesgo)	Oficina /Dirección	No aplica		
	5.3	CAUSA (S) DEL RIESGO ASIGNADO	No aplica			
	5.4	ALERTAS DE RIESGO (SEÑALES DE AVISO)	Incumplimiento de las normativas alineadas a la Ley de Gobierno Digital			
	5.5	RESPUESTA AL RIESGO	Elaboración y aprobación de Políticas de Seguridad de la Información alineadas a la NTP 27001 como inicio a la implementación del SGSI			

1. PROBABILIDAD DE OCURRENCIA	Muy Alta	0.90	0.045	0.090	0.180	0.360	0.720
	Alta	0.70	0.035	0.070	0.140	0.280	0.560
	Moderada	0.50	0.025	0.050	0.100	0.200	0.400
	Baja	0.30	0.015	0.030	0.060	0.120	0.240
	Muy Baja	0.10	0.005	0.010	0.020	0.040	0.080
2. IMPACTO EN LA EJECUCIÓN DE LA OBRA			0.05	0.10	0.20	0.40	0.80
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
3. PRIORIDAD DEL RIESGO					Baja	Moderada	Alta

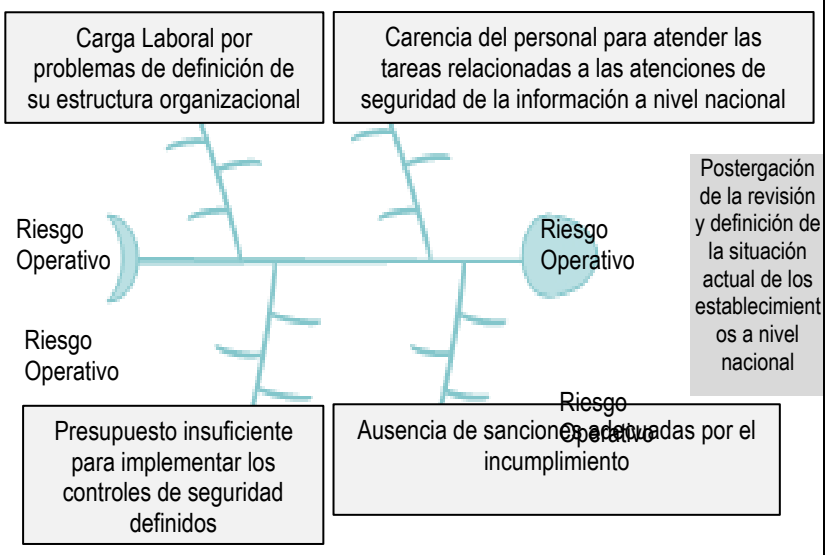
S06.01.01.02: Operaciones del SGSI (**)

FICHA DE RIESGO								
FICHA PARA IDENTIFICAR, ANALIZAR Y DAR RESPUESTA AL RIEGOS								
1	NOMBRE DEL PROCESO		Macroproceso (Nivel 0)	Gestión de Seguridad Integral, Emergencias y Desastres				
			Proceso (Nivel 1)	Gestión de Seguridad Informática				
			Subproceso (Nivel 2)	Seguridad de la Información				
			Procedimiento	Operaciones del SGSI				
			Actividad	Primera Fase: Informes técnicos de seguridad de información por dominios requeridos en la ISO NTP 27001				
2	OBJETIVO DEL PROCESO		Descripción	Primera Fase: Elaboración de informes técnicos de seguridad de información por dominios requeridos en la ISO NTP 27001.				
			Ubicación (Departamento, Ciudad Distrito)	Lima, Lima, Jesús María				
3	IDENTIFICACIÓN DE RIESGOS							
	3.1	TIPO DE RIESGO		Riesgo Operativo y Estratégico				
	3.2	CODIFICACION						
	3.3	DESCRIPCIÓN DEL RIESGO		Baja disponibilidad, riesgo de integridad y bajo control de acceso para confidencialidad de la información				
	3.4	CAUSA(S) GENERADORA(S)		Causa N° 1	Ausencia de Recursos Humanos			
				Causa N° 2	Falta de compromiso de alta dirección para la implementación de controles			
				Causa N° 3	Presupuesto insuficiente para implementar los controles de seguridad definidos			
				Causa N° 4	Ausencia de sanciones adecuadas por el incumplimiento			
		TECNICA DE DIAGRAMACION	Diagrama Causa Efecto	Diagrama de Ishikawa				
			Diagrama de Flujo de Procesos					
4		VALORACION DEL RIEGO						
	4.1	PROBABILIDAD DE OCURRENCIA				IMPACTO		
		Análisis Cualitativo	Análisis Cuantitativo			Análisis Cualitativo	Análisis Cuantitativo	
		Muy baja	0.10			Muy bajo	0.05	
		Baja	0.30			Bajo	0.10	
		Moderada	0.50			Moderado	0.20	
		Alta	0.70			Alto	0.40	
		Muy alta	0.90	0.90		Muy alto	0.80	0.80
		Muy Alta		0.90	0.90	**Muy Alto**		0.80

	4.3	PRIORIZACIÓN DEL RIESGO				
		Puntuación del Riesgo =Probabilidad x Impacto	0.72	Prioridad del Riesgo	Muy Alta Prioridad	
5	RESPUESTA A LOS RIESGOS					
	5.1	ESTRATEGIA	Mitigar Riesgo	X	Evitar Riesgo	
			Aceptar Riesgo		Transferir Riesgo	
	5.2	RIESGO ASIGNADO A (Solo después de haber marcado Transferir el Riesgo)	Oficina /Dirección	No aplica		
	5.3	CAUSA (S) DEL RIESGO ASIGNADO	No aplica			
	5.4	ALERTAS DE RIESGO (SEÑALES DE AVISO)	Incumplimiento de la información de los controles aplicados por dominios requeridos en la ISO NTP 27001			
	5.5	RESPUESTA AL RIESGO	Primera Fase: Elaboración de informes técnicos de seguridad de información por dominios aplicados y requeridos en la ISO NTP 27001			

1. PROBABILIDAD DE OCURRENCIA	Muy Alta	0.90	0.045	0.090	0.180	0.360	0.720
	Alta	0.70	0.035	0.070	0.140	0.280	0.560
	Moderada	0.50	0.025	0.050	0.100	0.200	0.400
	Baja	0.30	0.015	0.030	0.060	0.120	0.240
	Muy Baja	0.10	0.005	0.010	0.020	0.040	0.080
2. IMPACTO EN LA EJECUCIÓN DE LA OBRA			0.05	0.10	0.20	0.40	0.80
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
3. PRIORIDAD DEL RIESGO					Baja	Moderada	Alta

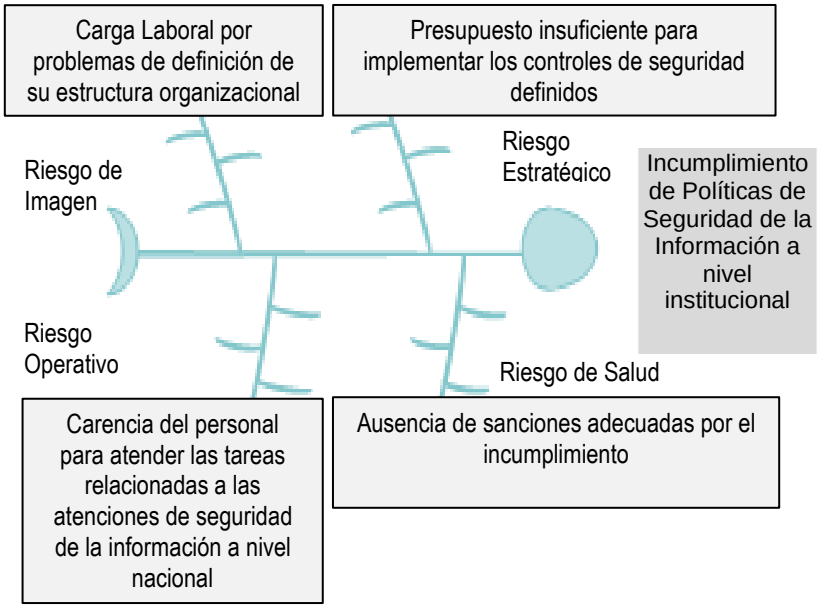
S06.01.01.03: Auditorias del SGSI (Visitas Inopinadas)(**)

FICHA DE RIESGO				
FICHA PARA IDENTIFICAR, ANALIZAR Y DAR RESPUESTA AL RIEGOS				
1	NOMBRE DEL PROCESO	Macroproceso (Nivel 0)	Gestión de Seguridad Integral, Emergencias y Desastres	
		Proceso (Nivel 1)	Gestión de Seguridad Informática	
		Subproceso (Nivel 2)	Seguridad de la Información	
		Procedimiento	Auditorias del SGSI (Visitas Inopinadas)	
		Actividad	Realizar el alineamiento de Seguridad de la Información en todos los establecimientos a nivel nacional	
2	OBJETIVO DEL PROCESO	Descripción	Mediante visitas inopinadas a los centros asistenciales, administrativos y de empresas que tienen contrato con EsSalud para verificar la aplicación de las medidas de seguridad de información	
		Ubicación (Departamento, Ciudad Distrito)	Lima, Lima, Jesús María	
3	IDENTIFICACIÓN DE RIESGOS			
	3.1 TIPO DE RIESGO		Riesgo Operativo	
	3.2 CODIFICACION			
	3.3 DESCRIPCIÓN DEL RIESGO		Postergación de la revisión y definición de la situación actual de los establecimientos a nivel nacional	
	3.4 CAUSA(S) GENERADORA(S)		Causa N° 1	Carga Laboral por problemas de definición de su estructura organizacional
			Causa N° 2	Carencia del personal para atender las tareas relacionadas a las atenciones de seguridad de la información a nivel nacional
			Causa N° 3	Presupuesto insuficiente para implementar los controles de seguridad definidos
			Causa N° 4	Ausencia de sanciones adecuadas por el incumplimiento
	TECNICA DE DIAGRAMACION	Diagrama Causa Efecto	Diagrama de Ishikawa	
		Diagrama de Flujo de Procesos		

4		VALORACION DEL RIEGO					
	4.1	PROBABILIDAD DE OCURRENCIA				IMPACTO	
		Análisis Cualitativo	Análisis Cuantitativo			Análisis Cualitativo	Análisis Cuantitativo	
		Muy baja	0.10			Muy bajo	0.05	
		Baja	0.30			Bajo	0.10	
		Moderada	0.50			Moderado	0.20	
		Alta	0.70			Alto	0.40	
		Muy alta	0.90	0.90		Muy alto	0.80	0.80
		Muy Alta		0.90	0.90	**Muy Alto**		
	4.3	PRIORIZACIÓN DEL RIESGO					
		Puntuación del Riesgo =Probabilidad x Impacto		**0.72**	Prioridad del Riesgo	**Muy Alta Prioridad**		
5		RESPUESTA A LOS RIESGOS					
	5.1	ESTRATEGIA		**Mitigar Riesgo**		**X**	**Evitar Riesgo**	
				Aceptar Riesgo			**Transferir Riesgo**	
	5.2	RIESGO ASIGNADO A (Solo después de haber marcado Transferir el Riesgo)		**Oficina /Dirección**	**No aplica**			
	5.3	CAUSA (S) DEL RIESGO ASIGNADO		**No aplica**				
	5.4	ALERTAS DE RIESGO (SEÑALES DE AVISO)		Incremento de los incidentes de seguridad a nivel nacional. No disminución de la brecha de seguridad de la información a nivel nacional.				
	5.5	RESPUESTA AL RIESGO		Programa de concientización para mejorar la cultura de seguridad de la información. Incrementar las visitas inopinadas para el acompañamiento en el levantamiento de observaciones.				

1. PROBABILIDAD DE OCURRENCIA	**Muy Alta**	**0.90**	**0.045**	**0.090**	**0.180**	**0.360**	**0.720**
	Alta	**0.70**	**0.035**	**0.070**	**0.140**	**0.280**	**0.560**
	Moderada	**0.50**	**0.025**	**0.050**	**0.100**	**0.200**	**0.400**
	Baja	**0.30**	**0.015**	**0.030**	**0.060**	**0.120**	**0.240**
	Muy Baja	**0.10**	**0.005**	**0.010**	**0.020**	**0.040**	**0.080**
2. IMPACTO EN LA EJECUCIÓN DE LA OBRA			**0.05**	**0.10**	**0.20**	**0.40**	**0.80**
			Muy Bajo	**Bajo**	**Moderado**	**Alto**	**Muy Alto**
3. PRIORIDAD DEL RIESGO					**Baja**	**Moderada**	**Alta**

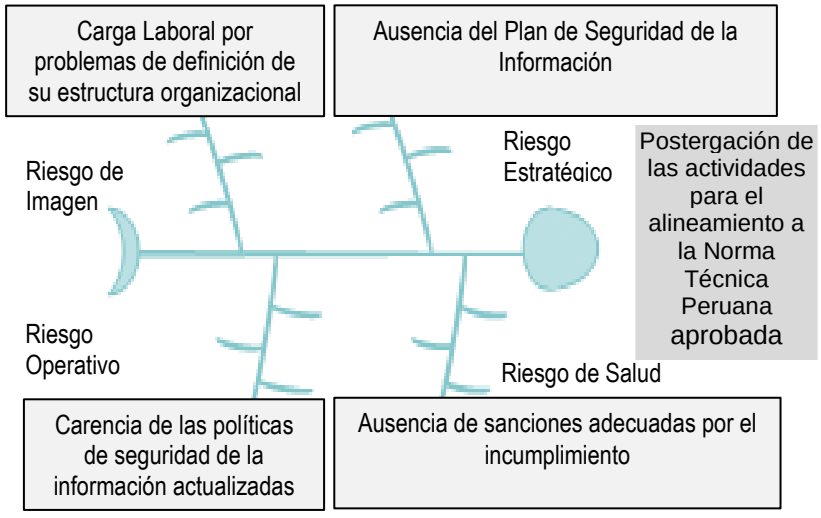
S06.01.01.04: Cumplimiento de Políticas de Seguridad de la Información

FICHA DE RIESGO					
FICHA PARA IDENTIFICAR, ANALIZAR Y DAR RESPUESTA AL RIEGOS					
1	NOMBRE DEL PROCESO	Macroproceso (Nivel 0)	Gestión de Seguridad Integral, Emergencias y Desastres		
		Proceso (Nivel 1)	Gestión de Seguridad Informática		
		Subproceso (Nivel 2)	Seguridad de la Información		
		Procedimiento	Cumplimiento de Políticas de Seguridad de la Información		
		Actividad	Cumplimiento de las políticas de seguridad de la información		
2	OBJETIVO DEL PROCESO	Descripción	Evaluar el cumplimiento de las políticas de seguridad de la información aprobadas a nivel nacional		
		Ubicación (Departamento, Ciudad Distrito)	Lima, Lima, Jesús María		
3	IDENTIFICACIÓN DE RIESGOS				
	3.1	TIPO DE RIESGO	Riesgo de Imagen Institucional, Operativo, Estratégico, de Salud		
	3.2	CODIFICACION			
	3.3	DESCRIPCIÓN DEL RIESGO	Incumplimiento de Políticas de Seguridad de la Información a nivel institucional		
	3.4	CAUSA(S) GENERADORA(S)	Causa N° 1	Carga Laboral por problemas de definición de su estructura organizacional	
			Causa N° 2	Carencia del personal para atender las tareas relacionadas a las atenciones de seguridad de la información a nivel nacional	
			Causa N° 3	Presupuesto insuficiente para implementar los controles de seguridad definidos	
			Causa N° 4	Ausencia de sanciones adecuadas por el incumplimiento	
		TECNICA DE DIAGRAMACION	Diagrama Causa Efecto	Diagrama de Ishikawa	
			Diagrama de Flujo de Procesos		

4		VALORACION DEL RIEGO					
	4.1	PROBABILIDAD DE OCURRENCIA				IMPACTO	
		Análisis Cualitativo	Análisis Cuantitativo		Análisis Cualitativo	Análisis Cuantitativo	
		Muy baja	0.10		Muy bajo	0.05	
		Baja	0.30		Bajo	0.10	
		Moderada	0.50		Moderado	0.20	
		Alta	0.70		Alto	0.40	
		Muy alta	0.90	0.90	Muy alto	0.80	0.80
		Muy alta		0.90	**Muy Alto**		0.80
	4.3	PRIORIZACIÓN DEL RIESGO					
		Puntuación del Riesgo =Probabilidad x Impacto		**0.72**	Prioridad del Riesgo	**Muy Alta Prioridad**	
5		RESPUESTA A LOS RIESGOS					
	5.1	ESTRATEGIA	**Mitigar Riesgo**		X	**Evitar Riesgo**	
			Aceptar Riesgo			**Transferir Riesgo**	
	5.2	RIESGO ASIGNADO A (Solo después de haber marcado Transferir el Riesgo)	**Oficina /Dirección**	**No aplica**			
	5.3	CAUSA (S) DEL RIESGO ASIGNADO	**No aplica**				
	5.4	ALERTAS DE RIESGO (SEÑALES DE AVISO)	Incumplimiento de las políticas de seguridad alineadas a la NTP-ISO 27001:2014 a nivel institucional				
	5.5	RESPUESTA AL RIESGO	Garantizar el cumplimiento a través de controles permanentes de las políticas de seguridad de la información en todos los establecimientos a nivel nacional				

1. PROBABILIDAD DE OCURRENCIA	**Muy Alta**	**0.90**	**0.045**	**0.090**	**0.180**	**0.360**	**0.720**
	Alta	**0.70**	**0.035**	**0.070**	**0.140**	**0.280**	**0.560**
	Moderada	**0.50**	**0.025**	**0.050**	**0.100**	**0.200**	**0.400**
	Baja	**0.30**	**0.015**	**0.030**	**0.060**	**0.120**	**0.240**
	Muy Baja	**0.10**	**0.005**	**0.010**	**0.020**	**0.040**	**0.080**
2. IMPACTO EN LA EJECUCIÓN DE LA OBRA			**0.05**	**0.10**	**0.20**	**0.40**	**0.80**
			Muy Bajo	**Bajo**	**Moderado**	**Alto**	**Muy Alto**
3. PRIORIDAD DEL RIESGO					**Baja**	**Moderada**	**Alta**

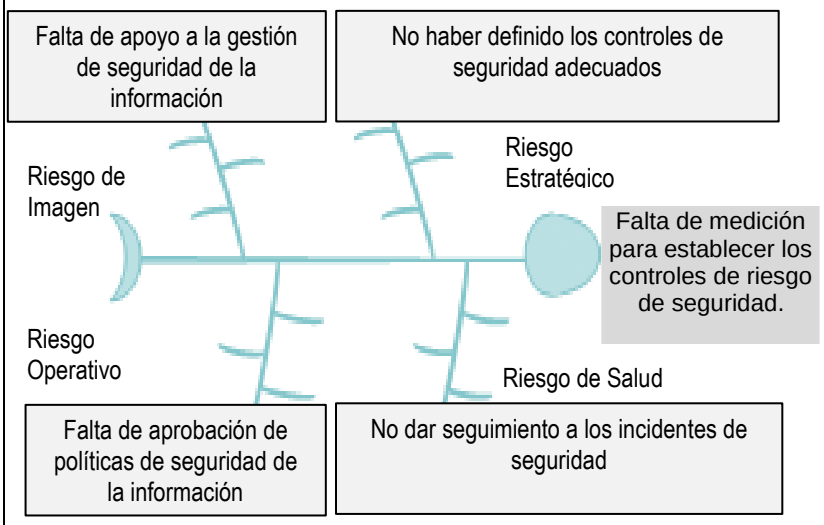
S06.01.01.05: Evaluación del alineamiento a la Norma Técnica Peruana aprobada por la Secretaria de Gobierno Digital

FICHA DE RIESGO							
FICHA PARA IDENTIFICAR, ANALIZAR Y DAR RESPUESTA AL RIEGOS							
1	NOMBRE DEL PROCESO		Macroproceso (Nivel 0)	Gestión de Seguridad Integral, Emergencias y Desastres			
			Proceso (Nivel 1)	Gestión de Seguridad Informática			
			Subproceso (Nivel 2)	Seguridad de la Información			
			Procedimiento	Alineamiento a la Norma Técnica Peruana			
			Actividad	Garantizar las actividades que conlleven al alineamiento a la Norma Técnica Peruana			
2	OBJETIVO DEL PROCESO		Descripción	Evaluación del alineamiento a la Norma Técnica Peruana aprobada por la Secretaria de Gobierno Digital			
			Ubicación (Departamento, Ciudad Distrito)	Lima, Lima, Jesús María			
3	IDENTIFICACIÓN DE RIESGOS						
	3.1	TIPO DE RIESGO		Riesgo de Imagen Institucional, Operativo, Estratégico, de Salud			
	3.2	CODIFICACION					
	3.3	DESCRIPCIÓN DEL RIESGO		Postergación de las actividades para el alineamiento a la Norma Técnica Peruana aprobada			
	3.4	CAUSA(S) GENERADORA(S)		Causa N° 1	Carga Laboral por problemas de definición de su estructura organizacional		
				Causa N° 2	Carencia de las políticas de seguridad de la información actualizadas		
				Causa N° 3	Ausencia del Plan de Seguridad de la Información		
				Causa N° 4	Ausencia de sanciones adecuadas por el incumplimiento		
		TECNICA DE DIAGRAMACION	Diagrama Causa Efecto	Diagrama de Ishikawa			
			Diagrama de Flujo de Procesos				
4		VALORACION DEL RIEGO					
	4.1	PROBABILIDAD DE OCURRENCIA				IMPACTO		
		Análisis Cualitativo	Análisis Cuantitativo			Análisis Cualitativo	Análisis Cuantitativo	
		Muy baja	0.10			Muy bajo	0.05	
		Baja	0.30			Bajo	0.10	
		Moderada	0.50			Moderado	0.20	
		Alta	0.70			Alto	0.40	
		Muy alta	0.90			Muy alto	0.80	
		Baja				**Alto**		

	4.3	PRIORIZACIÓN DEL RIESGO				
		Puntuación del Riesgo =Probabilidad x Impacto		Prioridad del Riesgo		
5	RESPUESTA A LOS RIESGOS					
	5.1	ESTRATEGIA	Mitigar Riesgo	X	Evitar Riesgo	
			Aceptar Riesgo		Transferir Riesgo	
	5.2	RIESGO ASIGNADO A (Solo después de haber marcado Transferir el Riesgo)	Oficina /Dirección	No aplica		
	5.3	CAUSA (S) DEL RIESGO ASIGNADO	No aplica			
	5.4	ALERTAS DE RIESGO (SEÑALES DE AVISO)	Ausencia de actividades que conlleven al alineamiento a la Norma Técnica Peruana			
	5.5	RESPUESTA AL RIESGO	Elaboración del plan de seguridad de la información para el alineamiento a la Norma Técnica Peruana aprobada por la Secretaria de Gobierno Digital			

1. PROBABILIDAD DE OCURRENCIA	Muy Alta	0.90	0.045	0.090	0.180	0.360	0.720
	Alta	0.70	0.035	0.070	0.140	0.280	0.560
	Moderada	0.50	0.025	0.050	0.100	0.200	0.400
	Baja	0.30	0.015	0.030	0.060	0.120	0.240
	Muy Baja	0.10	0.005	0.010	0.020	0.040	0.080
2. IMPACTO EN LA EJECUCIÓN DE LA OBRA			0.05	0.10	0.20	0.40	0.80
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
3. PRIORIDAD DEL RIESGO					Baja	Moderada	Alta

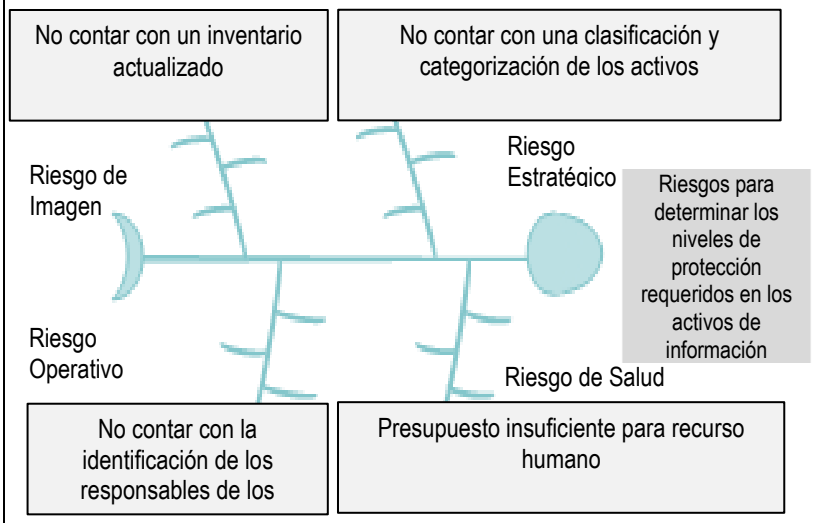
S06.01.01.06: Gestión de los riesgos en Seguridad de la Información

FICHA DE RIESGO							
FICHA PARA IDENTIFICAR, ANALIZAR Y DAR RESPUESTA AL RIEGOS							
1	NOMBRE DEL PROCESO		Macroproceso (Nivel 0)	Gestión de Seguridad Integral, Emergencias y Desastres			
			Proceso (Nivel 1)	Gestión de Seguridad Informática			
			Subproceso (Nivel 2)	Seguridad de la Información			
			Procedimiento	Gestión de los riesgos en Seguridad de la Información			
			Actividad	Mitigar los riesgos a partir de las vulnerabilidades identificadas			
2	OBJETIVO DEL PROCESO		Descripción	Mitigar los riesgos a partir de las vulnerabilidades identificadas a partir de la gestión eficiente de la matriz de riesgos de seguridad de la información			
			Ubicación (Departamento, Ciudad Distrito)	Lima, Lima, Jesús María			
3	IDENTIFICACIÓN DE RIESGOS						
	3.1	TIPO DE RIESGO		**Riesgo de Imagen Institucional, Operativo, Estratégico, de Salud**			
	3.2	CODIFICACION					
	3.3	DESCRIPCIÓN DEL RIESGO		Falta de medición para establecer los controles de riesgo de seguridad			
	3.4	CAUSA(S) GENERADORA(S)		Causa N° 1	Falta de apoyo a la gestión de seguridad de la información		
				Causa N° 2	Falta de aprobación de políticas de seguridad de la información		
				Causa N° 3	No haber definido los controles de seguridad adecuados		
				Causa N° 4	No dar seguimiento a los incidentes de seguridad		
		TECNICA DE DIAGRAMACION	Diagrama Causa Efecto	Diagrama de Ishikawa			
			Diagrama de Flujo de Procesos				
4		VALORACION DEL RIEGO					
	4.1	PROBABILIDAD DE OCURRENCIA				IMPACTO		
		Análisis Cualitativo	Análisis Cuantitativo			Análisis Cualitativo	Análisis Cuantitativo	
		Muy baja	0.10			Muy bajo	0.05	
		Baja	0.30			Bajo	0.10	
		Moderada	0.50			Moderado	0.20	
		Alta	0.70			Alto	0.40	
		Muy alta	0.90	0.90		Muy alto	0.80	0.80
		Muy alta		0.90		**Muy Alto**		0.80

	4.3	PRIORIZACIÓN DEL RIESGO				
		Puntuación del Riesgo =Probabilidad x Impacto	0.72	Prioridad del Riesgo	Muy Alta Prioridad	
5	RESPUESTA A LOS RIESGOS					
	5.1	ESTRATEGIA	Mitigar Riesgo	X	Evitar Riesgo	
			Aceptar Riesgo		Transferir Riesgo	
	5.2	RIESGO ASIGNADO A (Solo después de haber marcado Transferir el Riesgo)	Oficina /Dirección	No aplica		
	5.3	CAUSA (S) DEL RIESGO ASIGNADO	No aplica			
	5.4	ALERTAS DE RIESGO (SEÑALES DE AVISO)	Postergación de la atención de necesidades de seguridad de la información de la institución, reducción de presupuesto a las iniciativas de seguridad			
	5.5	RESPUESTA AL RIESGO	Medidas compensatorias para mitigar el riesgo de seguridad de la información			

1. PROBABILIDAD DE OCURRENCIA	Muy Alta	0.90	0.045	0.090	0.180	0.360	0.720
	Alta	0.70	0.035	0.070	0.140	0.280	0.560
	Moderada	0.50	0.025	0.050	0.100	0.200	0.400
	Baja	0.30	0.015	0.030	0.060	0.120	0.240
	Muy Baja	0.10	0.005	0.010	0.020	0.040	0.080
2. IMPACTO EN LA EJECUCIÓN DE LA OBRA			0.05	0.10	0.20	0.40	0.80
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
3. PRIORIDAD DEL RIESGO					Baja	Moderada	Alta

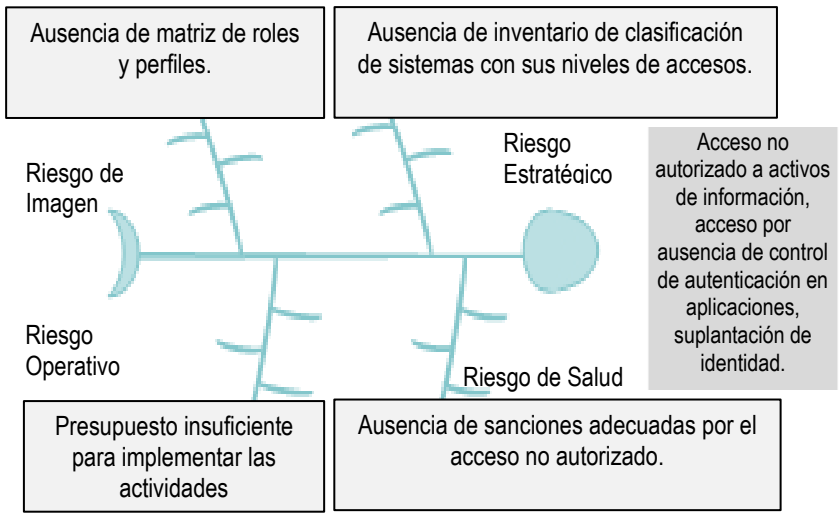
S06.01.01.07: Activos de Información

FICHA DE RIESGO							
FICHA PARA IDENTIFICAR, ANALIZAR Y DAR RESPUESTA AL RIEGOS							
1	NOMBRE DEL PROCESO		Macroproceso (Nivel 0)	Gestión de Seguridad Integral, Emergencias y Desastres			
			Proceso (Nivel 1)	Gestión de Seguridad Informática			
			Subproceso (Nivel 2)	Seguridad de la Información			
			Procedimiento	Clasificación de los Activos de Información			
			Actividad	Evaluar la matriz de activos de información de EsSalud			
2	OBJETIVO DEL PROCESO		Descripción	Elaboración y evaluación de la matriz de activos de información de EsSalud para una óptima gestión de los mismos			
			Ubicación (Departamento, Ciudad Distrito)	Lima, Lima, Jesús María			
3	IDENTIFICACIÓN DE RIESGOS						
	3.1	TIPO DE RIESGO		**Riesgo de Imagen Institucional, Operativo, Estratégico, de Salud**			
	3.2	CODIFICACION					
	3.3	DESCRIPCIÓN DEL RIESGO		Riesgos para determinar los niveles de protección requeridos en los activos de información			
	3.4	CAUSA(S) GENERADORA(S)		Causa N° 1	No contar con un inventario actualizado		
				Causa N° 2	No contar con la identificación de los responsables de los activos		
				Causa N° 3	No contar con una clasificación y categorización de los activos		
				Causa N° 4	Presupuesto insuficiente para recurso humano		
		TECNICA DE DIAGRAMACION	Diagrama Causa Efecto	Diagrama de Ishikawa			
			Diagrama de Flujo de Procesos					
4		VALORACION DEL RIEGO					
	4.1	PROBABILIDAD DE OCURRENCIA				IMPACTO		
		Análisis Cualitativo	Análisis Cuantitativo			Análisis Cualitativo	Análisis Cuantitativo	
		Muy baja	0.10			Muy bajo	0.05	
		Baja	0.30			Bajo	0.10	
		Moderada	0.50			Moderado	0.20	
		Alta	0.70			Alto	0.40	
		Muy alta	0.90	0.90		Muy alto	0.80	0.80
		Muy alta		0.90		**Muy Alto**		0.80

	4.3	PRIORIZACIÓN DEL RIESGO				
		Puntuación del Riesgo =Probabilidad x Impacto	0.72	Prioridad del Riesgo	Muy Alta Prioridad	
5	RESPUESTA A LOS RIESGOS					
	5.1	ESTRATEGIA	Mitigar Riesgo	X	Evitar Riesgo	
			Aceptar Riesgo		Transferir Riesgo	
	5.2	RIESGO ASIGNADO A (Solo después de haber marcado Transferir el Riesgo)	Oficina /Dirección	No aplica		
	5.3	CAUSA (S) DEL RIESGO ASIGNADO	No aplica			
	5.4	ALERTAS DE RIESGO (SEÑALES DE AVISO)	Explotación de vulnerabilidades en los activos de información por falta de controles adecuados según criticidad			
	5.5	RESPUESTA AL RIESGO	Elaboración y evaluación de la matriz de activos de información de EsSalud para una óptima gestión de los mismos			

1. PROBABILIDAD DE OCURRENCIA	Muy Alta	0.90	0.045	0.090	0.180	0.360	0.720
	Alta	0.70	0.035	0.070	0.140	0.280	0.560
	Moderada	0.50	0.025	0.050	0.100	0.200	0.400
	Baja	0.30	0.015	0.030	0.060	0.120	0.240
	Muy Baja	0.10	0.005	0.010	0.020	0.040	0.080
2. IMPACTO EN LA EJECUCIÓN DE LA OBRA			0.05	0.10	0.20	0.40	0.80
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
3. PRIORIDAD DEL RIESGO					Baja	Moderada	Alta

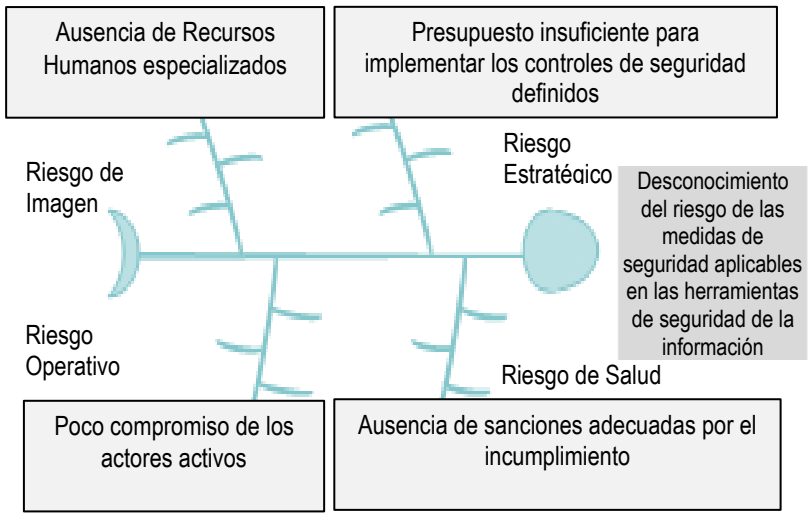
S06.01.02.01.01: Control de Accesos

FICHA DE RIESGO							
FICHA PARA IDENTIFICAR, ANALIZAR Y DAR RESPUESTA AL RIEGOS							
1	NOMBRE DEL PROCESO	Macroproceso (Nivel 0)	Gestión de Seguridad Integral, Emergencias y Desastres				
		Proceso (Nivel 1)	Gestión de Seguridad Informática				
		Subproceso (Nivel 2)	Seguridad Informática				
		Subproceso (Nivel 3)	Control de Accesos				
		Procedimiento	Gestión en el control de accesos				
		Actividad	Realizar el control de accesos y seguimiento a las actividades realizadas				
2	OBJETIVO DEL PROCESO	Descripción	Realizar el control de accesos y seguimiento a las actividades realizadas por parte del proveedor de servicios de operación de las herramientas de seguridad				
		Ubicación (Departamento, Ciudad Distrito)	Lima, Lima, Jesús María				
3	IDENTIFICACIÓN DE RIESGOS						
	3.1	TIPO DE RIESGO	Riesgo de Imagen Institucional, Operativo, Estratégico, de Salud				
	3.2	CODIFICACION					
	3.3	DESCRIPCIÓN DEL RIESGO	Acceso no autorizado a activos de información, acceso no autorizado por ausencia de control de autenticación en aplicaciones, suplantación de identidad.				
	3.4	CAUSA(S) GENERADORA(S)	Causa N° 1	Ausencia de matriz de roles y perfiles.			
			Causa N° 2	Ausencia de inventario de clasificación de sistemas con sus niveles de accesos.			
			Causa N° 3	Presupuesto insuficiente para implementar las actividades necesarias.			
			Causa N° 4	Ausencia de sanciones adecuadas por el acceso no autorizado.			
		TECNICA DE DIAGRAMACION	Diagrama Causa Efecto	Diagrama de Ishikawa			
			Diagrama de Flujo de Procesos				
4		VALORACION DEL RIEGO					
	4.1	PROBABILIDAD DE OCURRENCIA				IMPACTO		
		Análisis Cualitativo	Análisis Cuantitativo			Análisis Cualitativo	Análisis Cuantitativo	
		Muy baja	0.10			Muy bajo	0.05	
		Baja	0.30			Bajo	0.10	
		Moderada	0.50			Moderado	0.20	
		Alta	0.70			Alto	0.40	
		Muy alta	0.90	0.90		Muy alto	0.80	0.80
		Muy alta		0.90		**Muy Alto**		0.80

	4.3	PRIORIZACIÓN DEL RIESGO				
		Puntuación del Riesgo =Probabilidad x Impacto	0.72	Prioridad del Riesgo	Muy Alta Prioridad	
5	RESPUESTA A LOS RIESGOS					
	5.1	ESTRATEGIA	Mitigar Riesgo	X	Evitar Riesgo	
			Aceptar Riesgo		Transferir Riesgo	
	5.2	RIESGO ASIGNADO A (Solo después de haber marcado Transferir el Riesgo)	Oficina /Dirección	No aplica		
	5.3	CAUSA (S) DEL RIESGO ASIGNADO	No aplica			
	5.4	ALERTAS DE RIESGO (SEÑALES DE AVISO)	Falta de control de accesos y seguimiento a las actividades realizadas por parte del proveedor de servicios de operación de las herramientas de seguridad y accesos no autorizados a los sistemas de información			
	5.5	RESPUESTA AL RIESGO	Realizar el control de accesos y seguimiento a las actividades realizadas por parte del proveedor de servicios de operación de las herramientas de seguridad y accesos no autorizados a los sistemas de información			

1. PROBABILIDAD DE OCURRENCIA	Muy Alta	0.90	0.045	0.090	0.180	0.360	0.720
	Alta	0.70	0.035	0.070	0.140	0.280	0.560
	Moderada	0.50	0.025	0.050	0.100	0.200	0.400
	Baja	0.30	0.015	0.030	0.060	0.120	0.240
	Muy Baja	0.10	0.005	0.010	0.020	0.040	0.080
2. IMPACTO EN LA EJECUCIÓN DE LA OBRA			0.05	0.10	0.20	0.40	0.80
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
3. PRIORIDAD DEL RIESGO					Baja	Moderada	Alta

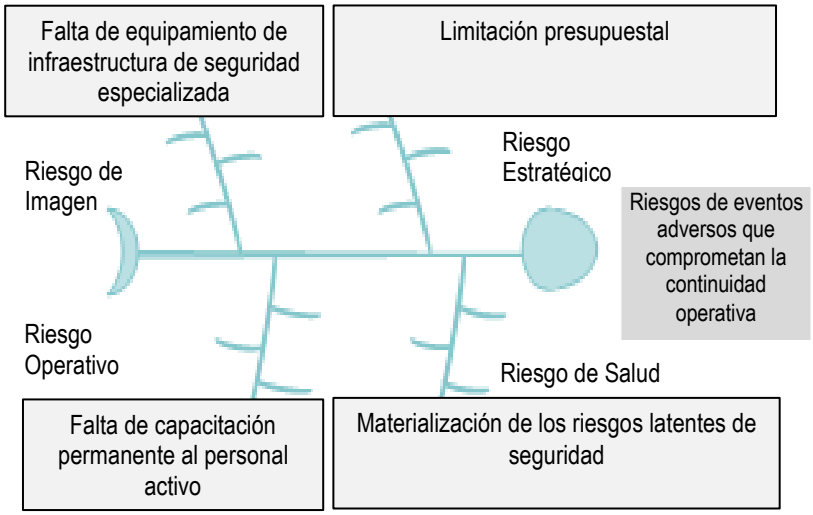
S06.01.02.01.02: Aplicación de políticas de seguridad perimetral y de la red de datos institucional

FICHA DE RIESGO								
FICHA PARA IDENTIFICAR, ANALIZAR Y DAR RESPUESTA AL RIEGOS								
1	NOMBRE DEL PROCESO		Macroproceso (Nivel 0)	Gestión de Seguridad Integral, Emergencias y Desastres				
			Proceso (Nivel 1)	Gestión de Seguridad Informática				
			Subproceso (Nivel 2)	Seguridad Informática				
			Subproceso (Nivel 3)	Aplicación de políticas de seguridad perimetral y de la red de datos institucional				
			Procedimiento	Aplicación de las políticas y configuraciones				
			Actividad	Implementación de conjunto de políticas y configuraciones				
2	OBJETIVO DEL PROCESO		Descripción	Determinar la aplicación de las políticas y configuraciones de la seguridad perimetral y de la red de datos institucional				
			Ubicación (Departamento, Ciudad Distrito)	Lima, Lima, Jesús María				
3	IDENTIFICACIÓN DE RIESGOS							
	3.1	TIPO DE RIESGO		Riesgo de Imagen Institucional, Operativo, Estratégico, de Salud				
	3.2	CODIFICACION						
	3.3	DESCRIPCIÓN DEL RIESGO		Desconocimiento del riesgo de las medidas de seguridad aplicables en las herramientas de seguridad de la información				
	3.4	CAUSA(S) GENERADORA(S)		Causa N° 1	Ausencia de Recursos Humanos especializados			
				Causa N° 2	Poco compromiso de los actores			
				Causa N° 3	Presupuesto insuficiente para implementar los controles de seguridad definidos			
				Causa N° 4	Ausencia de sanciones adecuadas por el incumplimiento			
		TECNICA DE DIAGRAMACION	Diagrama Causa Efecto	Diagrama de Ishikawa				
			Diagrama de Flujo de Procesos					
4		VALORACION DEL RIEGO						
	4.1	PROBABILIDAD DE OCURRENCIA					IMPACTO		
		Análisis Cualitativo	Análisis Cuantitativo				Análisis Cualitativo	Análisis Cuantitativo	
		Muy baja	0.10				Muy bajo	0.05	
		Baja	0.30				Bajo	0.10	
		Moderada	0.50				Moderado	0.20	
		Alta	0.70				Alto	0.40	
		Muy alta	0.90	0.90			Muy alto	0.80	0.80
		Muy alta		0.90			**Muy Alto**		0.80

	4.3	PRIORIZACIÓN DEL RIESGO				
		Puntuación del Riesgo =Probabilidad x Impacto	0.72	Prioridad del Riesgo	Muy Alta Prioridad	
5	RESPUESTA A LOS RIESGOS					
	5.1	ESTRATEGIA	Mitigar Riesgo	X	Evitar Riesgo	
			Aceptar Riesgo		Transferir Riesgo	
	5.2	RIESGO ASIGNADO A (Solo después de haber marcado Transferir el Riesgo)	Oficina /Dirección	No aplica		
	5.3	CAUSA (S) DEL RIESGO ASIGNADO	No aplica			
	5.4	ALERTAS DE RIESGO (SEÑALES DE AVISO)	Explotación de vulnerabilidades en los activos de información por falta de controles adecuados según criticidad			
	5.5	RESPUESTA AL RIESGO	Elaboración y evaluación de la matriz de activos de información de EsSalud para una óptima gestión de los mismos			

1. PROBABILIDAD DE OCURRENCIA	Muy Alta	0.90	0.045	0.090	0.180	0.360	0.720
	Alta	0.70	0.035	0.070	0.140	0.280	0.560
	Moderada	0.50	0.025	0.050	0.100	0.200	0.400
	Baja	0.30	0.015	0.030	0.060	0.120	0.240
	Muy Baja	0.10	0.005	0.010	0.020	0.040	0.080
2. IMPACTO EN LA EJECUCIÓN DE LA OBRA			0.05	0.10	0.20	0.40	0.80
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
3. PRIORIDAD DEL RIESGO					Baja	Moderada	Alta

S06.01.02.02.03: Gestión de Incidentes

FICHA DE RIESGO								
FICHA PARA IDENTIFICAR, ANALIZAR Y DAR RESPUESTA AL RIEGOS								
1	NOMBRE DEL PROCESO		Macroproceso (Nivel 0)	Gestión de Seguridad Integral, Emergencias y Desastres				
			Proceso (Nivel 1)	Gestión de Seguridad Informática				
			Subproceso (Nivel 2)	Seguridad Informática				
			Subproceso (Nivel 3)	Gestión de Incidentes				
			Procedimiento	Gestión de Incidentes				
			Actividad	Garantizar la continuidad operativa				
2	OBJETIVO DEL PROCESO		Descripción	Elaborar actividades que garanticen la continuidad operativa a partir de la óptima gestión de incidentes				
			Ubicación (Departamento, Ciudad Distrito)	Lima, Lima, Jesús María				
3	IDENTIFICACIÓN DE RIESGOS							
	3.1	TIPO DE RIESGO		**Riesgo de Imagen Institucional, Operativo, Estratégico, de Salud**				
	3.2	CODIFICACION						
	3.3	DESCRIPCIÓN DEL RIESGO		Riesgos de eventos adversos que comprometan la continuidad operativa				
	3.4	CAUSA(S) GENERADORA(S)		Causa N° 1	Falta de equipamiento de infraestructura de seguridad especializada			
				Causa N° 2	Falta de capacitación permanente al personal activo			
				Causa N° 3	Limitación presupuestal			
				Causa N° 4	Materialización de los riesgos latentes de seguridad			
		TECNICA DE DIAGRAMACION	Diagrama Causa Efecto	Diagrama de Ishikawa				
			Diagrama de Flujo de Procesos					
4		VALORACION DEL RIEGO						
	4.1	PROBABILIDAD DE OCURRENCIA					IMPACTO		
		Análisis Cualitativo	Análisis Cuantitativo				Análisis Cualitativo	Análisis Cuantitativo	
		Muy baja	0.10				Muy bajo	0.05	
		Baja	0.30				Bajo	0.10	
		Moderada	0.50				Moderado	0.20	
		Alta	0.70				Alto	0.40	
		Muy alta	0.90	0.90			Muy alto	0.80	0.80
		Muy alta		0.90			**Muy Alto**		0.80

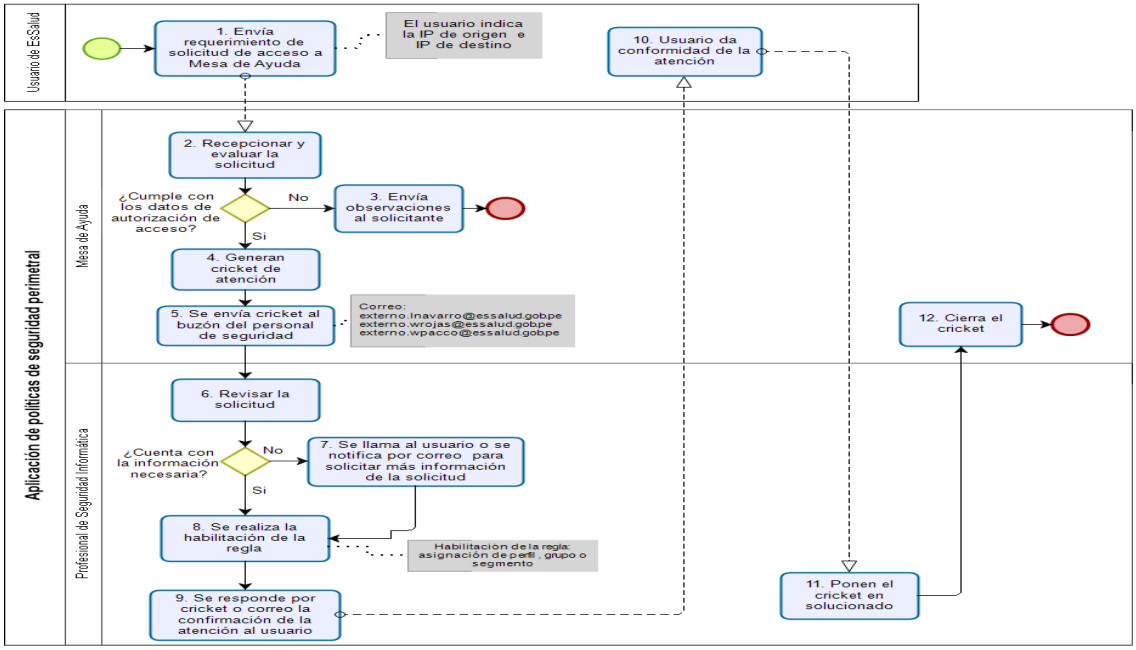
	4.3	PRIORIZACIÓN DEL RIESGO				
		Puntuación del Riesgo =Probabilidad x Impacto	0.72	Prioridad del Riesgo	Muy Alta Prioridad	
5	RESPUESTA A LOS RIESGOS					
	5.1	ESTRATEGIA	Mitigar Riesgo	X	Evitar Riesgo	
			Aceptar Riesgo		Transferir Riesgo	
	5.2	RIESGO ASIGNADO A (Solo después de haber marcado Transferir el Riesgo)	Oficina /Dirección	No aplica		
	5.3	CAUSA (S) DEL RIESGO ASIGNADO	No aplica			
	5.4	ALERTAS DE RIESGO (SEÑALES DE AVISO)	Incidentes de seguridad, obsolescencia tecnológica.			
	5.5	RESPUESTA AL RIESGO	Respuesta temprana a Incidentes de seguridad y medidas compensatorias para mitigar el riesgo tecnológico.			

1. PROBABILIDAD DE OCURRENCIA	Muy Alta	0.90	0.045	0.090	0.180	0.360	0.720
	Alta	0.70	0.035	0.070	0.140	0.280	0.560
	Moderada	0.50	0.025	0.050	0.100	0.200	0.400
	Baja	0.30	0.015	0.030	0.060	0.120	0.240
	Muy Baja	0.10	0.005	0.010	0.020	0.040	0.080
2. IMPACTO EN LA EJECUCIÓN DE LA OBRA			0.05	0.10	0.20	0.40	0.80
			Muy Bajo	Bajo	Moderado	Alto	Muy Alto
3. PRIORIDAD DEL RIESGO					Baja	Moderada	Alta

10. Procesos Críticos

La Oficina de Seguridad Informática, que depende de la Gerencia Central de Tecnologías de la Información y Comunicaciones, tiene a su cargo la Seguridad de Información y Seguridad Informática. En el presente manual, se ha identificado el siguiente proceso crítico "Aplicación de políticas de seguridad perimetral y de la red de datos institucional" a cargo de la Seguridad de la Información, cuyo objetivo es realizar la Determinar la aplicación de las políticas y configuraciones de la seguridad perimetral y de la red de datos institucional.

A continuación, se muestra el diagrama de flujo del proceso de "Aplicación de políticas de seguridad perimetral y de la red de datos institucional".



11. Oportunidades de mejora

En el punto anterior se ha descrito el proceso crítico, en el cual se observó algunas oportunidades de mejora en cuanto a la organización, sistemas informáticos y documentación. Para minimizar el impacto negativo que estas podrían ocasionar, se ha planteado las siguientes mejoras:

a. Implementar un sistema integrado de información de los procesos y acciones operativas, que permita evaluar la operación continúa de los servicios configurados en las herramientas de seguridad; así como también el seguimiento de las observaciones encontradas.
b. Acciones de control que evitará la dispersión de la información y asegurará la trazabilidad. Así mismo permitirá el control de calidad de los proyectos desarrollados en GCTIC.
c. Gestionar el proceso de privilegios y gestión de accesos e identidades de los sistemas de información, servicios informáticos y plataformas tecnológicas a nivel nacional, a fin que los usuarios de acuerdo a los accesos y perfiles otorgados y validados por la Sede Central no tengan acceso a la información no autorizada gestionada por las herramientas de seguridad. (Acceso restringidos)
d. Actualizar las normas de seguridad informática que permita el mantenimiento la integridad, disponibilidad, confidencialidad de la información manejada a través de las herramientas de seguridad; asimismo la elaboración de las políticas, estándares y procedimientos de seguridad informática y la gestión de su cumplimiento de acuerdo a las normas vigentes en gestión de operación de servicios.

La Oficina de Seguridad Informática, debe de elaborar y hacer aprobar el Plan General de Seguridad Informática, el cual, permita entender las vulnerabilidades en las herramientas de seguridad, para una vez detectadas, tomar las medidas necesarias para prevenir esos problemas. Asimismo, ayudar a proteger los datos y los sistemas críticos, ajustados a la legislación vigente y a la Ley de Protección de Datos.

12. Aspectos Finales

12.1 Conclusiones

1. Se ha detectado que existen actividades que se realizan en la Gerencia de Producción y no están incluidas formalmente en el ROF correspondiente.
2. Como se aprecia en el documento, la Oficina de Seguridad Informática tiene un rol clave en el desempeño de EsSalud al establecer las políticas e instrumentos de su competencia, como el Plan General de Seguridad de la Información, gestión de recursos de seguridad, estándares de información, entre otros aspectos importantes. Dentro de sus responsabilidades se encuentran la gestión del plan de seguridad de información, así como la coordinación de esfuerzos entre el personal de sistemas y los empleados de las áreas de negocios, siendo éstos últimos los responsables de la información que utiliza.
3. La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.
4. Por tanto, mientras la seguridad de la información integra toda la información independientemente del medio en que este, la seguridad informática únicamente atiende a la protección de las instalaciones informáticas y de la información en medios digitales
5. Actualmente los procesos de Seguridad Informática están a cargo de la Gerencia de Producción.

12.2 Recomendaciones

1. Debido a que la Gerencia Central de Tecnologías de Información y Comunicaciones no cuenta con una Oficina de Seguridad de la Información, la cual desarrolle el rol de auditor y que en diferentes ocasiones el rol es asumido por la Oficina de Seguridad Informática, se recomienda la implementación la Oficina de Seguridad de la Información. Ésta no deberá estar incluida en la Gerencia Central de Tecnologías de Información y Comunicaciones. Se recomienda que la Oficina de Seguridad de la Información, según la NTP-ISO/IEC 27001 en la Cláusula 5.3 y el control A6.1.1, donde mencionan que los documentos deben ser elevados a la Alta Dirección, este ubicada al nivel de la GCTIC.
2. Se recomienda actualizar de manera constante el presente manual para poder recoger cambios o mejoras internas de los procesos descritos.
3. Se recomienda publicar el presente manual en el Portal de Transparencia Estándar de EsSalud, para que sirva como guía a todos los interesados en conocer los procesos descritos de la Seguridad Informática.
4. Se sugiere que la Oficina de Seguridad de información será la encargada de garantizar la integridad, disponibilidad y confidencialidad de los activos de información y el uso adecuado de los Sistemas de Información y Herramientas de Seguridad, brindando las disposiciones y lineamientos de seguridad que deben cumplir todos los usuarios respecto al uso de los Sistemas de Información de ESSALUD.