PROCEDIMIENTO	Código: **S03.03.02.03**
	Versión: 01
	Vigencia: 24/09/2025
Dueño del proceso: Oficina de Administración	

RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

	Nombres y Apellidos	Cargo	Firma y Sello
Elaborado por:	Manuel Aguilar Cori	Oficial de Seguridad y Confianza Digital	Firmado digitalmente por: AGUILAR CORI Manuel Isidro FAU 20380799643 hard Fecha: 23/09/2025 15:01:24
	Víctor Chávez Gómez	Jefe de Tecnologías de la Información	Firmado digitalmente por: CHAVEZ GOMEZ Victor Hugo FAU 20380799643 soft Fecha: 23/09/2025 18:27:06
Revisado por:	Apolinar Madrid Escobar	Jefe (dt) de la Oficina de Planeamiento y Presupuesto	Firmado digitalmente por: MADRID ESCOBAR Apolinar Junior FAU 20380799643 hard Fecha: 23/09/2025 16:34:56
Aprobado por:	Alberto Blas Ortiz	Jefe de la Oficina de Administración	

Versión	Descripción de Cambios (indicar sección de corresponder)	Fecha
01	Versión inicial	24/09/2025

1. BASE LEGAL

1.1. ISO/IEC 27001:2022 “Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de Seguridad de la Información – Requisitos” (en adelante ISO/IEC 27001).
1.2. NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de Seguridad de la Información – Requisitos (en adelante NTP-ISO/IEC 27001).
1.3. ISO/IEC 27002 “Seguridad de la Información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información” (en adelante ISO/IEC 27002).
1.4. NTP-ISO/IEC 27002:2022 “Seguridad de la Información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información” (en adelante NTP-ISO/IEC 27002).
1.5. Versión Actualizada de la Directiva N° 02-2015-SERVIR/GPGSC Régimen Disciplinario y Procedimiento Sancionador de la Ley N° 30057, Ley del Servicio Civil.
1.6. Reglamento Interno de los Servidores Civiles - RIS de la Agencia de Promoción de la Inversión Privada – PROINVERSIÓN.
1.7. Código de Ética de la Agencia de la Promoción de la Inversión Privada PROINVERSIÓN.

2. DEFINICIONES Y SIGLAS

2.1. Definiciones

2.1.1. **Activo de Información:** Información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que puede ser entendida, compartida y usada. Es de valor para la empresa y tiene un ciclo de vida.

2.1.2. **Ciberseguridad:** Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.

2.1.3. **Confidencialidad:** Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.

2.1.4. **Disponibilidad:** Propiedad de ser accesible y utilizable por petición de una entidad autorizada.

2.1.5. **Evento o Suceso:** Ocurrencia o cambio de un conjunto particular de circunstancias.
Nota 1: Un evento puede ser una o más ocurrencias, y puede tener varias causas.
Nota 2: Un evento puede consistir en algo que no sucede.
Nota 3: Un evento a veces puede ser referido como un "incidente " o "accidente”.

2.1.6. **Evento de Seguridad de Información**: Ocurrencia identificada de un sistema, servicio o el estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación antes desconocida que puede ser la seguridad relevante.

2.1.7. **Gestión de Incidentes de Seguridad de Información:** Aseguramiento que el acceso lógico a los activos de información está autorizado y Procesos para detectar, informar, evaluar, responder frente a, y aprender de incidentes de seguridad de la información.

2.1.8. **Incidente de Seguridad**: Es un evento adverso que puede generar un impacto en un sistema de información o en una red de servicios informáticos comprometiendo la confidencialidad, integridad y disponibilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o acciones de amenaza que puedan poner en riesgo los mecanismos de seguridad existentes.

2.1.9. **Incidente de Seguridad de Información**: Evento único o una serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

2.1.10. **Integridad:** Propiedad de exactitud y lo completo.

2.1.11. **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Nota 1: Además, otras propiedades, como la autenticidad, la responsabilidad, el no repudio, y confiabilidad también pueden estar involucrados.

2.1.12. **Sistema de Gestión:** Conjunto de elementos interrelacionados o que interactúan en una organización para establecer políticas, objetivos y procesos, para lograr esos objetivos.

Nota 1: Un sistema de gestión puede abordar una sola disciplina o varias disciplinas.
Nota 2: Los elementos del sistema incluyen la estructura de la organización, funciones y responsabilidades, la planificación, operación, etc.
Nota 3: El alcance de un sistema de gestión puede incluir la totalidad de la organización, específico y funciones identificadas en la organización, las secciones específicas e identificadas de la organización, o uno o más funciones a través de un grupo de organizaciones.

2.1.13. **Sistema de Gestión de la Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

2.1.14. **Usuario Responsable del Servicio Tercerizado:** responsable del servicio, es quien tiene requerimientos del negocio a ser atendidos por un tercero.

2.2. Siglas:

- CGTD: Comité de Gobierno y Transformación Digital.
- SGSI: Sistema de Gestión de Seguridad de la Información.
- OSCD: Oficial de Seguridad y Confianza Digital.
- ETRIS: Equipo Técnico de Respuestas ante Incidentes de Seguridad.

3. RESPONSABILIDADES

3.1. Del Oficial de Seguridad y Confianza Digital (OSCD)

3.1.1. Evaluar el evento/incidente y registrar la información.
3.1.2. Comunicar, el incidente al personal que reportó el incidente, a los propietarios de los activos de información afectados y a los colaboradores y terceros que correspondan (entre ellos Centro Nacional de Seguridad Digital - PCM).
3.1.3. Establecer una cadena de custodia y no eliminar ninguna evidencia o registro relacionado al incidente.
3.1.4. Registrar las acciones inmediatas ejecutadas para detener el impacto del incidente de seguridad de la información.
3.1.5. Proponer alternativas de solución al incidente y ejecutar la más adecuada.
3.1.6. Verificar que los activos afectados vuelvan a su condición operativa.
3.1.7. Realizar coordinaciones con el Equipo Técnico de Respuestas ante Incidentes de Seguridad y con el Equipo de Apoyo de Respuestas ante Incidentes de Seguridad.
3.1.8. Implementar y mantener controles de seguridad de la información que puedan responder de manera efectiva a los incidentes cuando se identifiquen.
3.1.9. Planificar y realizar la revisión de cumplimiento de controles.

3.2. De las áreas usuarias de PROINVERSION

3.2.1. Reportar los eventos/incidentes de seguridad de la información a través de los canales correspondientes.
3.2.2. Cumplir con los lineamientos establecidos para el manejo de incidentes de seguridad de la información.

3.3. Del Especialista de respuestas ante Incidentes de Seguridad

3.3.1. Resolver incidencias de la infraestructura tecnológica, aplicaciones y seguridad física o coordinar con los terceros que brindan servicios la resolución de incidencias de acuerdo con el servicio prestado a PROINVERSIÓN.

3.3.2. Proponer alternativas de solución a incidentes de seguridad de la información.

3.3.3. Implementar y mantener controles de seguridad de la información en la infraestructura tecnológica y aplicaciones que puedan responder de manera efectiva a los incidentes cuando se identifiquen.

3.3.4. Comunicar los incidentes de seguridad de la información

3.4. Del Especialista de tecnologías de información externo

3.4.1. Resolver incidencias de la infraestructura tecnológica o aplicaciones coordinar con los especialistas de respuesta ante incidencias de seguridad la resolución de incidencias de acuerdo con el servicio prestado a PROINVERSIÓN.

4. GENERALIDADES

4.1. Para el registro y gestión de los incidentes de seguridad de la información se utiliza el documento FORMATO Reporte de Incidentes de Seguridad de la Información.

4.2. Para el seguimiento y control de los incidentes de seguridad de la información se utiliza el documento FORMATO Control de Incidentes de Seguridad de la Información.

4.3. La documentación de la solución de los incidentes sirve para retroalimentar y fortalecer el proceso de gestión de incidentes de seguridad de la información, para lo cual se utiliza el documento FORMATO Lecciones Aprendidas de Seguridad de la Información.

4.4. Entre los especialistas del Equipo Técnico de Respuestas ante Incidentes de Seguridad se encuentran los colaboradores del:

- Área de Tecnologías de la Información:
  - Oficial de Seguridad y Confianza Digital, para resolver incidencias de seguridad de la información y ciberseguridad, quien lo lidera.
  - Infraestructura, para resolver incidencias informáticas, en servidores, equipos de telecomunicación, entre otros.
  - Soporte Técnico, para resolver las incidencias informáticas en estaciones de trabajo.
  - Desarrollo de Sistemas, para resolver incidencias en aplicaciones y bases de datos.
- Colaboradores de la Oficina de Administración, para resolver incidencias de seguridad física, servicios generales.

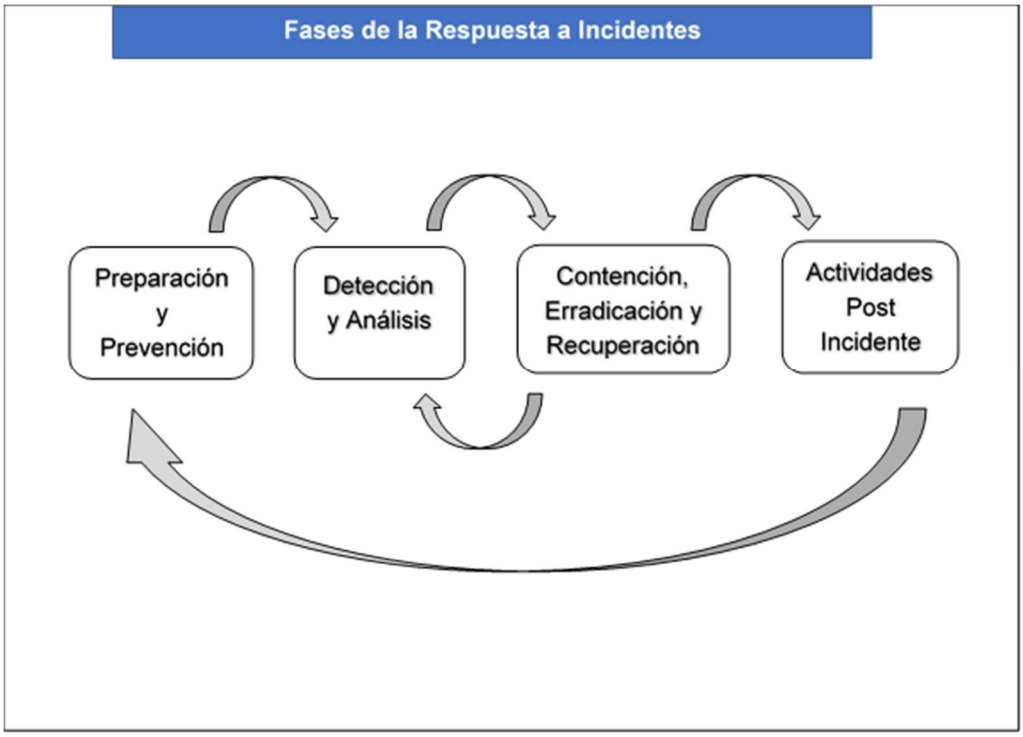
4.5. El Equipo de Apoyo de Respuestas ante Incidentes de Seguridad está conformado por:

- Jefe del Área de Tecnologías de la Información, quien lo lidera.
- Jefe del Área de Logística
- Jefe de la Oficina de Administración

4.6. La comunicación y reporte periódico o inmediato respecto a la gestión de incidentes de seguridad de la información la realiza principalmente el OSCD, a través de correo electrónico, verbal (telefónico, presencial) o plataforma indicada por el tercero (entre ellos Centro Nacional de Seguridad Digital - PCM).

4.7. La gestión de riesgos, para el caso de incidentes de seguridad de la información se debe realizar según los lineamientos definidos de Gestión de Riesgos de Seguridad de la Información.

4.8. Dentro de la gestión de incidentes de seguridad de la información de PROINVERSIÓN, se identifican 4 fases que definen claramente el procedimiento a seguir después de que se presente un evento que afecte a la seguridad de la información:



5. SECUENCIA DE ACTIVIDADES

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Analizar evento de seguridad de la información			
1	Analizar evento de seguridad de la información - Evaluar el evento con la finalidad de determinar si corresponde o no a un incidente de seguridad de la información de acuerdo con lo definido en la **Tabla N° 2 "Tipo y Categoría de Incidentes de Seguridad de la Información" (Anexo N° 02)**.	Área de TI.	OSCD
2	Calificar evento de seguridad de la información Sino es un incidente de seguridad de la información, se da por terminado el procedimiento ¿Califica como incidente de seguridad de la información? Si: Ir a la tarea 3 No: Termina proceso.	Área de TI.	OSCD
Registrar incidente de seguridad de la información			
3	Registrar incidente de seguridad de la información - Si es un incidente de seguridad de la información, debe registrar el incidente en el punto "1. Reporte y Registro" y "2. Datos del Incidente - Tipo y Categoría de Incidente" del documento **Anexo N° 06 Reporte de Incidentes de Seguridad de la Información**.	Área de TI.	OSCD
4	Evaluar incidente de seguridad de la información - Evaluar el incidente y registrar la información correspondiente en el punto "2. Datos del Incidente", del documento **Anexo N° 6 Reporte de Incidentes de Seguridad de la Información** y, en el documento **Anexo N° 7 Control de Incidentes de Seguridad de la Información**. - La especificación del tipo y categoría del activo la realiza de acuerdo con lo definido en la **Tabla N° 3 "Lista de Activos de Información" (Anexo N° 03)**. - La determinación de la gravedad y prioridad de atención del incidente la realiza de acuerdo con lo definido en la **Tabla N° 4 "Gravedad y Prioridad de Incidentes" (Anexo N° 04)**.	Área de TI.	OSCD
5	Comunicar Incidente de seguridad de la información - Comunicar, vía correo electrónico, el incidente al personal que reportó el incidente, a los	Área de TI.	OSCD

	propietarios de los activos de información afectados, al Equipo de Apoyo de Respuestas ante Incidentes de Seguridad y a los colaboradores que considere necesarios.		
Solucionar incidente de seguridad de la información			
6	Registrar Acciones Inmediatas Tomadas - De corresponder, debe registrar las acciones inmediatas ejecutadas para detener el impacto del incidente de seguridad de la información en el punto "5. Acciones Inmediatas", del documento **Anexo N° 06 Reporte de Incidentes de Seguridad de la Información.**	Área de TI.	Especialista de Respuestas ante Incidentes de Seguridad
7	Investigar Incidente de seguridad de la información - Realizar la determinación de las causas e identificar el impacto del incidente y las registran en el punto "6. Investigación del Incidente", del documento **Anexo N° 06 Reporte de Incidentes de Seguridad de la Información**.	Área de TI. Oficina de Administración.	Especialista de Respuestas ante Incidentes de Seguridad
8	Recolectar Evidencias del incidente de seguridad de la información - Establecer una cadena de custodia y no se elimina ninguna evidencia o registro relacionado al incidente hasta que este se haya cerrado; esto lo registran en el punto "7. Evidencias del Incidente", del documento **Anexo N° 06 Reporte de Incidentes de Seguridad de la Información**.	Área de TI.	Especialista de Respuestas ante Incidentes de Seguridad
9	Evaluar si se requiere escalar el Incidente - En caso el incidente de seguridad de la información no pueda ser resuelto internamente y el impacto del incidente lo amerita, escalar el incidente a los Contactos Externos en seguridad de la información con los que cuente PROINVERSIÓN ¿Se requiere escalar atención del incidente? Si: Ir a la tarea 10 No: Ir a la tarea 11	Área de TI.	Especialista de Respuestas ante Incidentes de Seguridad
10	Atender incidente de seguridad de la información con recurso interno	Área de TI.	Especialista de Respuestas ante Incidentes de Seguridad
Solucionar incidente con recurso externo			
11	Atender incidente de seguridad de la información con recurso externo	Área de TI.	Especialista de Tecnologías de Información Externo
12	Elaborar informe de atención de incidente de seguridad de la información con recurso externo	Área de TI.	Especialista de Tecnologías de Información Externo
Documentar incidente de seguridad de la información			
13	Verificar solución de Incidente de seguridad de la información Verificar que los activos afectados vuelvan a su condición operativa ¿Se encontró solución satisfactoria del incidente? Si: Ir a tarea 14 No: Ir a tarea 10	Área de TI.	OSCD
Evaluar mejora continua de la seguridad de la información			
14	Evaluar si se requiere mejora continua **Anexo N° 9 Lecciones Aprendidas de Seguridad de la Información** Verificar si se considera pertinente realizar una acción correctiva o no, así mismo registrar las lecciones aprendidas del incidente Si: Ir a tarea 15 No: Ir a tarea 16	Área de TI.	OSCD
15	Registrar acción correctiva - De considerarlo pertinente, principalmente para un análisis más exhaustivo del mismo, de las causas del incidente u otro tema relacionado, se debe registrar una solicitud de acción de mejora en el documento **Anexo N° 08 Solicitud de Acción Correctiva y de Mejora (SACM) del SGSI**	Área de TI.	OSCD
Comunicar resolución de incidente de seguridad de la información			
16	Documentar atención de incidente de seguridad de la información, incluido registro de acciones correctivas y de mejora.	Área de TI.	OSCD

17	Comunicar resolución de incidente de seguridad de la información Comunicar los resultados (que se encontró solución satisfactoria), vía correo electrónico, al colaborador o Usuario Responsable que reportó el incidente. En caso el incidente de seguridad requiera que se apliquen las acciones disciplinarias a colaboradores o en caso de terceros que presten servicios se deban aplicar las acciones legales/contractuales pertinentes.	Área de TI.	OSCD
Fin			

6. ANEXOS

6.1. Anexo 01 : Tabla N° 1 “Canales de Atención de Eventos e Incidentes de Seguridad de la Información”
6.2. Anexo 02 : Tabla N° 2 “Tipo y Categoría de Incidente de Seguridad de la Información”
6.3. Anexo 03 : Tabla N° 3 “Lista de Activos de Información”
6.4. Anexo 04 : Tabla N° 4 “Gravedad y Prioridad de Incidentes”
6.5. Anexo 05 : Flujograma de procedimiento de respuesta a incidentes de seguridad de la información
6.6. Anexo 06 : Reporte de Incidentes de Seguridad de la Información.
6.7. Anexo 07 : Control de Incidentes de Seguridad de la Información.
6.8. Anexo 08 : Solicitud de Acción Correctiva y de Mejora (SACM) del SGSI
6.9. Anexo 09 : Lecciones Aprendidas de Seguridad de la Información.

Anexo N° 01
Tabla N° 1 "Canales de Atención de Eventos e Incidentes de Seguridad de la Información"

CORREO	segurinfo@proinversion.gob.pe
APLICACIÓN	http://mesadeayuda.proinversion.gob.pe
Horario de Atención Lunes a viernes: 09:00 am. – 05:00 pm. Sábados, Domingos y fuera de los horarios establecidos comunicarse solo a segurinfo@proinversion.gob.pe	

Anexo N° 02 : Tabla N° 2 "Tipo y Categoría de Incidente de Seguridad de la Información"

TIPO	CÓDIGO	CATEGORÍA
Acceso y uso de la información	ISI001	Accesos lógicos no autorizados respecto al correo electrónico, internet, file server, ftp u otros servicios tecnológicos
	ISI002	Acceso físico no autorizado a los recursos o instalaciones de **PROINVERSIÓN** sin la autorización debida
	ISI003	Uso inadecuado de la información contenida en los recursos tecnológicos de **PROINVERSIÓN**
	ISI004	Uso inadecuado de la información contenida en los recursos no tecnológicos de **PROINVERSIÓN** (medios físicos)
	ISI005	Divulgación no autorizada de información física
	ISI006	Divulgación no autorizada de información digital
Custodia de la información	ISI007	Pérdida de la información (en forma física) en servicios, equipos o instalaciones
	ISI008	Pérdida de la información (en forma digital) en servicios, equipos o instalaciones
	ISI009	Robo de información digital
	ISI010	Robo de información física
	ISI011	Destrucción no autorizada de información en formato físico
	ISI012	Destrucción no autorizada de información en formato digital
Custodia de activos de información	ISI013	Robo de teléfonos celulares inteligentes, tabletas o laptops que han sido asignados a colaboradores de **PROINVERSIÓN**
	ISI014	Mal uso de los activos que **PROINVERSIÓN** le brinda, para usos personales y no a los que fueron originalmente destinados (cumplimiento de funciones)
	ISI015	Daño físico sobre los equipos de tecnología de información de **PROINVERSIÓN**
Falla en las operaciones	ISI016	Falla o sobrecarga de los sistemas de Información (situaciones que generan la indisponibilidad)
	ISI017	Falla o sobrecarga de las comunicaciones (situaciones que generan la indisponibilidad)
Cambios operacionales y en aplicaciones	ISI018	Modificación no autorizada de un sitio o página web de **PROINVERSIÓN**
	ISI019	Instalación o eliminación no autorizada de software
	ISI020	Cambios no controlados en el software
	ISI021	Cambios no controlados en la infraestructura tecnológica
Hacking / Infiltración lógica	ISI022	Ataques de ingeniería social (phishing)
	ISI023	Ataques de denegación de servicio o bloqueo de acceso
	ISI024	Ataque o infección por código malicioso (virus, gusanos, troyanos, otros)
	ISI025	Alteración no autorizada de un sitio o página web de **PROINVERSIÓN**
	ISI026	Vigilancia y espionaje
	ISI027	Ataques a OWASP sitios web
Desastres	ISI028	Desastres naturales (sismos, inundaciones, otros)
	ISI029	Desastres no naturales (incendios, derrumbes por mala construcción, otros)
	ISI030	Incidentes de terrorismo
Otro	ISI031	Compromiso de datos personales
	ISI032	Otro - Especificar

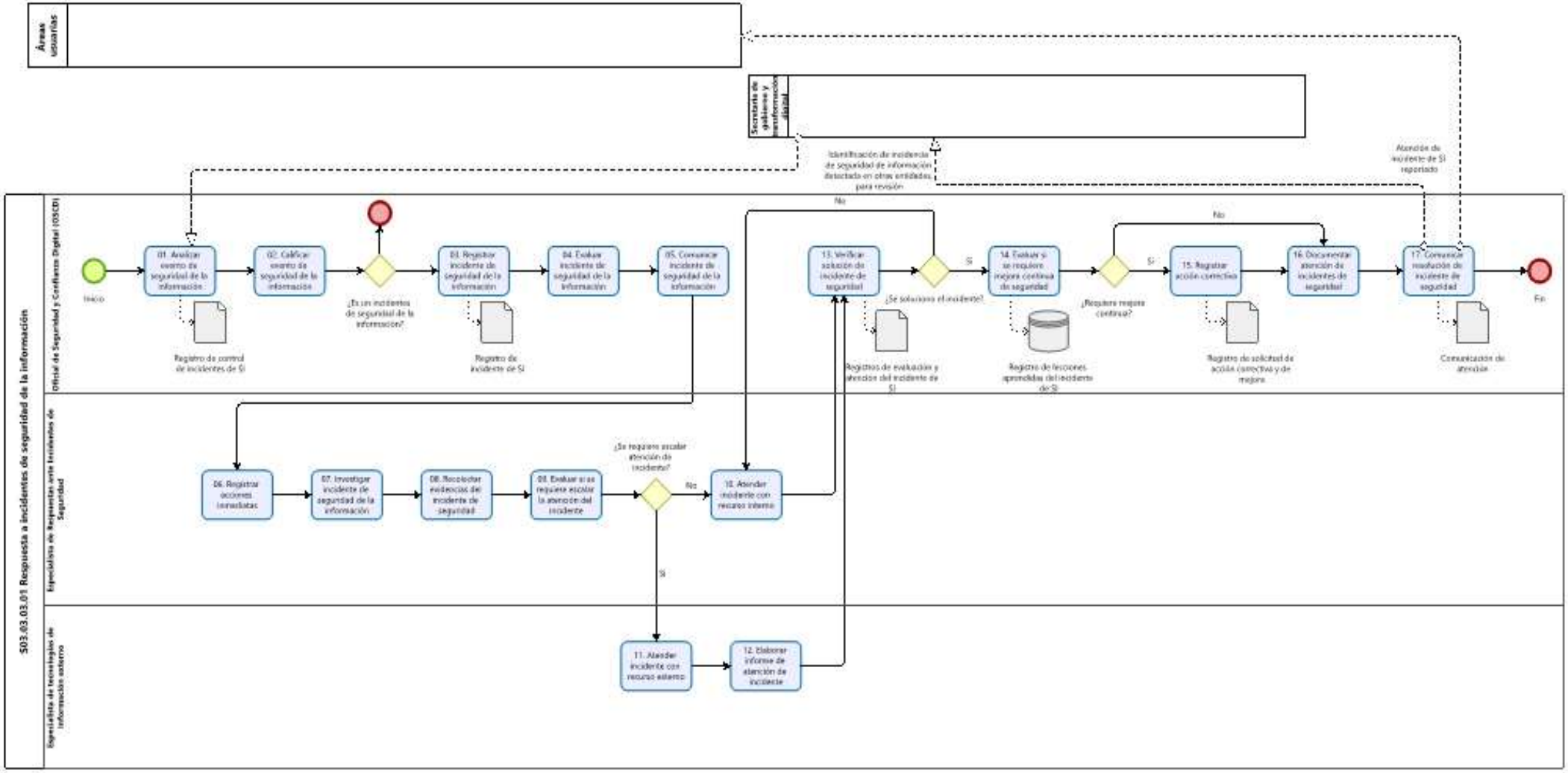
Anexo N° 03 : Tabla N° 3 "Lista de Activos de Información"

TIPO	CATEGORÍA	GUÍA REFERENCIAL
Información	Electrónica	Documentos digitales Bases de datos
	Impresa	Documentos en físico (impresos)
	Electrónica e Impresa	Documentos
Software	Software comercial	Software base o sistema operativo Antivirus Manejador de base de datos
	Software desarrollado por terceros	Aplicativos desarrollados por terceros
	Software desarrollado internamente	Aplicativos desarrollados por colaboradores de PROINVERSIÓN
	Otro software	Software libre
Físico	Equipo de procesamiento	Equipo de cómputo Laptop Equipo móvil Servidor físico
	Equipo virtual de cómputo	Servidor virtual
	Equipo de comunicación	Switch Router
	Instalaciones	Centro de Datos
	Contenedor de documentos	Carpetas compartidas Files Archivadores
	Medio de almacenamiento removible	USB Disco duro externo
	Otro equipo	Token
Personas	Responsables de tomar decisiones (Directores, Gerentes, Jefes, entre otros)	Directores Gerentes Jefes
	Otro personal	Demás colaboradores de PROINVERSIÓN
Servicios	Servicios públicos	Energía Eléctrica Telecomunicaciones
	Procesamiento y comunicaciones	Housing
	Otros servicios	Courier

Anexo N° 04
Tabla N° 4 "Gravedad y Prioridad de Incidentes"

GRAVEDAD DEL INCIDENTE	DESCRIPCIÓN	PRIORIDAD DE ATENCIÓN
No Significativo	En **PROINVERSIÓN**: Afecta la confidencialidad, integridad o disponibilidad de uno o más activos de información no confidenciales ni restringidos causando interrupción mínima de las operaciones, procesos o actividades. Adicionalmente: - No origina incumplimiento de Objetivos o - No origina incumplimiento de Obligaciones ni pérdidas económicas o - No origina Perjuicio a la reputación o - No origina Divulgación no autorizada de datos personales o - No origina daños personales.	3
Moderadamente Significativo	En **PROINVERSIÓN**: Afecta la confidencialidad, integridad o disponibilidad de uno o más activos de información confidenciales o restringidos causando interrupción moderada de las operaciones, procesos o actividades. Adicionalmente: - No origina incumplimiento de Objetivos y/u - Origina Incumplimiento mínimo de Obligaciones ni pérdidas económicas y/u - Origina Perjuicio mínimo a la reputación y/u - Origina Divulgación no autorizada de datos personales o - No origina daños personales.	2
Significativo	Afecta la confidencialidad, integridad o disponibilidad de uno o más activos de información confidenciales causando interrupción significativa de las operaciones, procesos o actividades. Adicionalmente: - Origina Incumplimiento significativo de Objetivos y/u - Origina Incumplimiento significativo de Obligaciones y pérdidas económicas y/u - Origina Perjuicio mayor a la reputación y/u - Origina Divulgación no autorizada de datos personales y/u - Origina daños personales.	1

Anexo N° 05 : "Flujograma de procedimiento de respuesta a incidentes de seguridad de la información"



Anexo N° 06 : "Reporte de incidentes de seguridad de la información"

PRO INVERSIÓN	FORMATO	Código:
	REPORTE DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 00
		Vigencia:

1. REPORTE Y REGISTRO					
CÓDIGO DEL INCIDENTE	I00x-año		TICKET		
FECHA	xx/xx/xxxx		HORA		
TIPO DE COMUNICACIÓN					
CORREO			TELÉFONO		
DATOS DEL REPORTANTE					
NOMBRES Y APELLIDOS			CÓDIGO		
CARGO			UNIDAD ORGÁNICA		
CORREO ELECTRÓNICO			TELÉFONO Y ANEXO		
OBSERVACIONES					
2. DATOS DEL INCIDENTE					
TIPO DE INCIDENTE		CATEGORÍA DEL INCIDENTE			
DESCRIPCIÓN DEL INCIDENTE					
UNIDAD ORGÁNICA DONDE SE PRODUJO EL INCIDENTE					
USUARIO(S) INVOLUCRADOS(S) EN LA OCURRENCIA DEL INCIDENTE	CÓDIGO / DNI	NOMBRES Y APELLIDOS		UNIDAD ORGÁNICA / EMPRESA	
ACTIVOS DE INFORMACIÓN AFECTADOS O COMPROMETIDOS					
NOMBRE	DETALLE	PROPIETARIO	TIPO	CATEGORÍA	UBICACIÓN ESPECÍFICA
DURACIÓN DEL INCIDENTE	INICIO	FECHA		HORA	
	FIN	FECHA		HORA	
GRAVEDAD DEL INCIDENTE		PRIORIDAD DE ATENCIÓN		#N/D	
3. ESPECIALISTAS					
N°	NOMBRES Y APELLIDOS		CARGO		UNIDAD ORGÁNICA / EMPRESA
ESPECIALISTA RESPONSABLE					
OTROS ESPECIALISTAS					
4. COMUNICADOS					
N°	NOMBRES Y APELLIDOS		CARGO		UNIDAD ORGÁNICA / EMPRESA
PROPIETARIOS DE ACTIVOS DE INFORMACIÓN AFECTADOS Y/O COMPROMETIDOS					
OTROS COLABORADORES					
5. ACCIONES INMEDIATAS (DE CORRESPONDER)					
N°	DESCRIPCIÓN ACCIÓN TOMADA			FECHA	

6. INVESTIGACIÓN DEL INCIDENTE

NOMBRE DEL ACTIVO DE INFORMACIÓN AFECTADO O COMPROMETIDO	AMENAZA	VULNERABILIDAD	CAUSAS	PROBABILIDAD	¿QUÉ PRINCIPIO DEL ACTIVO DE INFORMACIÓN ES AFECTADO POR LA AMENAZA?							IMPACTO	SEVERIDAD CUANTITATIVA	SEVERIDAD CUALITATIVA	CONTROLES DEFICIENTES
					C		I		D		VALOR CID				
														#N/D	
														#N/D	
														#N/D	

7. EVIDENCIAS DEL INCIDENTE

8. ESCALAMIENTO DEL INCIDENTE

FECHA		HORA	
RESPONSABLE		EMPRESA	
COMENTARIOS			

9. ALTERNATIVAS DE SOLUCIÓN AL INCIDENTE

10. CIERRE DEL INCIDENTE

FECHA DE CIERRE		HORA DE CIERRE	
SOLUCIÓN IMPLEMENTADA	SOLUCIÓN		
	ACTIVIDADES RELEVANTES		
CONTROLES NUEVOS / MEJORADOS			
SANCIONES	COORDINACIÓN DE SANCIONES / ACCIONES LEGALES - CONTRACTUALES	¿SE RECOMENDARON SANCIONES U OTRAS ACCIONES?	
		COLABORADOR CON QUE SE COORDINÓ	
		COMENTARIOS	
	¿APLICARON SANCIONES U OTRAS ACCIONES?		
	SANCIONES (SEGÚN REGLAMENTO INTERNO DE TRABAJO) / OTRAS ACCIONES		
	COMENTARIOS		
LECCIONES APRENDIDAS			
RESPONSABLE DE LA SOLUCIÓN			
	UNIDAD ORGÁNICA / EMPRESA		
CONFORMIDAD DE LA SOLUCIÓN DEL INCIDENTE			

Anexo N° 07
"Control de Incidentes de Seguridad de la Información"

PRO INVERSIÓN	FORMATO	Código:
	CONTROL DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 00
		Vigencia:

Fecha de Actualización:

REPORTE Y REGISTRO DEL INCIDENTE					INICIO INCIDENTE				INFORMACIÓN DE INCIDENTE				SEGUIMIENTO INCIDENTE				FIN DEL INCIDENTE					
CÓDIGO	TICKET	FECHA	HORA	REPORTADO POR	TIPO	CATEGORÍA	FECHA	HORA	DESCRIPCIÓN DEL INCIDENTE	UNIDAD ORGÁNICA DONDE SE PRODUJO EL INCIDENTE	GRAVEDAD DEL INCIDENTE	PRIORIDAD DE ATENCIÓN	RESPONSABLE DEL SEGUIMIENTO	RESPONSABLE DE LA SOLUCIÓN	ESTADO DE ATENCIÓN	COMENTARIOS / OBSERVACIONES	FECHA	HORA	¿SE IMPLEMENTARON O MEJORARON CONTROLES?	¿SE APLICARON SANCIONES U OTRAS ACCIONES?	¿SE REGISTRARON LAS LECCIONES APRENDIDAS?	CONFORMIDAD DE LA SOLUCIÓN DEL INCIDENTE

Anexo N° 08 : "Solicitud de Acción Correctiva y de Mejora (SACM) del SGSI"

PRO INVERSIÓN	FORMATO		Código: XXX-XXX-XXXX
	SOLICITUD DE ACCIÓN CORRECTIVA Y DE MEJORA (SACM) DEL SGSI		Versión: 01
			Vigencia: xx/xx/2025
	Planeamiento y Modernización Institucional	Modernización Institucional	Página 1 de 1

INFORMACIÓN INICIAL (A LLENAR POR EL SOLICITANTE)			
NOMBRE DEL SOLICITANTE		FECHA	
CARGO		N°	000x-SACM 2025
NOMBRE DEL PROCESO		N° DE REFERENCIA	

ORIGEN DE LA SACM

- ☐ Resultados de Auditorías
- ☐ Observación del personal
- ☐ Análisis de Riesgos
- ☐ Revisión de la Gestión
- ☐ Evaluación de Requisitos
- ☐ Resultados de Incidentes
- ☐ Otros (especificar)

ACCIÓN NECESARIA

- ☐ Acción Correctiva (AC)
- ☐ Oportunidad de Mejora (OM)

NORMA(S) ASOCIADA(S) AL HALLAZGO ISO/IEC 27001 y NTP-ISO/IEC 27001 (Requisito xxxx)

DESCRIPCIÓN DEL HALLAZGO - NO CONFORMIDAD (NC) / OBSERVACIÓN (OB) / OPORTUNIDAD DE MEJORA (OM)

ANÁLISIS DE CAUSAS Y ACCIONES A TOMAR

IDENTIFICACIÓN Y ANÁLISIS DE LA CAUSA

FECHA DE ANÁLISIS		RESPONSABLE	

PLAN DE ACCIÓN

ACCIÓN INMEDIATA (SÓLO PARA CASOS QUE APLIQUE)

ACCIÓN CORRECTIVA

ACTIVIDAD	RESPONSABLE	FECHA		ESTADO	EVIDENCIA
		PLANIFICADA	EJECUTADA		
RESPONSABLE DEL SEGUIMIENTO	(Oficial de Seguridad y Confianza Digital)		FECHA DE CIERRE PROPUESTA		xx/xx/xxxx
REQUIERE MODIFICAR ANÁLISIS DE RIESGOS		☐ SI		☐ NO	
SE CUMPLIERON LAS ACCIONES PROPUESTAS		☐ SI		☐ NO	

VERIFICACIÓN DE LA EFICACIA DEL PLAN DE ACCIÓN

FECHA		RESPONSABLE	(Oficial de Seguridad y Confianza Digital)
EVALUACIÓN			

☐ EFECTIVA ☐ NO EFECTIVA **NOTA:** Si no es efectiva aperture otra SACM y coloque en N° DE REFERENCIA el N° de SACM

Cierre de SACM

☐ SI ☐ NO

Anexo N° 09 : "Lecciones aprendidas de Seguridad de la Información"

PRO INVERSIÓN	FORMATO	Código:
	LECCIONES APRENDIDAS DE SEGURIDAD DE LA INFORMACIÓN	Versión: 00
		Vigencia:

Fecha de Actualización:

DESCRIPCIÓN DEL INCIDENTE	CAUSAS DEL INCIDENTE	IMPACTO DEL INCIDENTE	ACTIVIDADES PARA SOLUCIONAR EL INCIDENTE	TIEMPO ESTIMADO DE ATENCIÓN	REFERENCIA A DOCUMENTOS RELACIONADOS A LA SOLUCIÓN