1. Objetivo

Establecer las actividades a seguir para gestionar los incidentes de seguridad informática y/o seguridad de la información, con la finalidad de proteger a los/las usuarios/as de amenazas que vulneren su información.

2. Base Legal

2.1 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 Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

2.2 Decreto Supremo Nº 005-2013-MC, que aprueba el Reglamento de Organización y Funciones del Ministerio de Cultura.

2.3 Decreto de Urgencia Nº 007-2020, que aprueba el marco de confianza digital y dispone medidas para su fortalecimiento (literal i del numeral 7.4 del artículo 7).

3. Requerimientos

3.1 Matriz de Evaluación y decisión de incidentes de seguridad actualizado por el/la Oficial de Seguridad de la Información.

4. Detalle del Procedimiento

N° DE ACTIVIDAD	ÓRGANO O UNIDAD ORGÁNICA/ RESPONSABLE	ACCIÓN A SEGUIR
1	Órgano o Unidad Orgánica/ Usuario/a	**Comunicar suceso de Seguridad.-** Remite especificaciones del evento/incidente de seguridad, siguiendo los pasos establecidos en el MP-OGETIC-OIT-13 Gestión de incidencias y/o requerimientos de Mesa de ayuda.
2	OIT/ Analista de Mesa de Ayuda	**Derivar suceso de Seguridad.-** Analizar el suceso de seguridad e identificar si corresponde a un evento, incidente o debilidad de seguridad de acuerdo a la “Matriz de decisión de Incidentes de Seguridad”. Se deberá recopilar todas las evidencias necesarias sobre el suceso de seguridad reportado y registrarlas o adjuntarlas en el aplicativo de mesa de ayuda. Tipo de Suceso: • Evento: Continua en paso 3. • Incidente de Seguridad de la Información: Continua en paso 4. • Incidente de Seguridad Informática: Continua en paso 6.

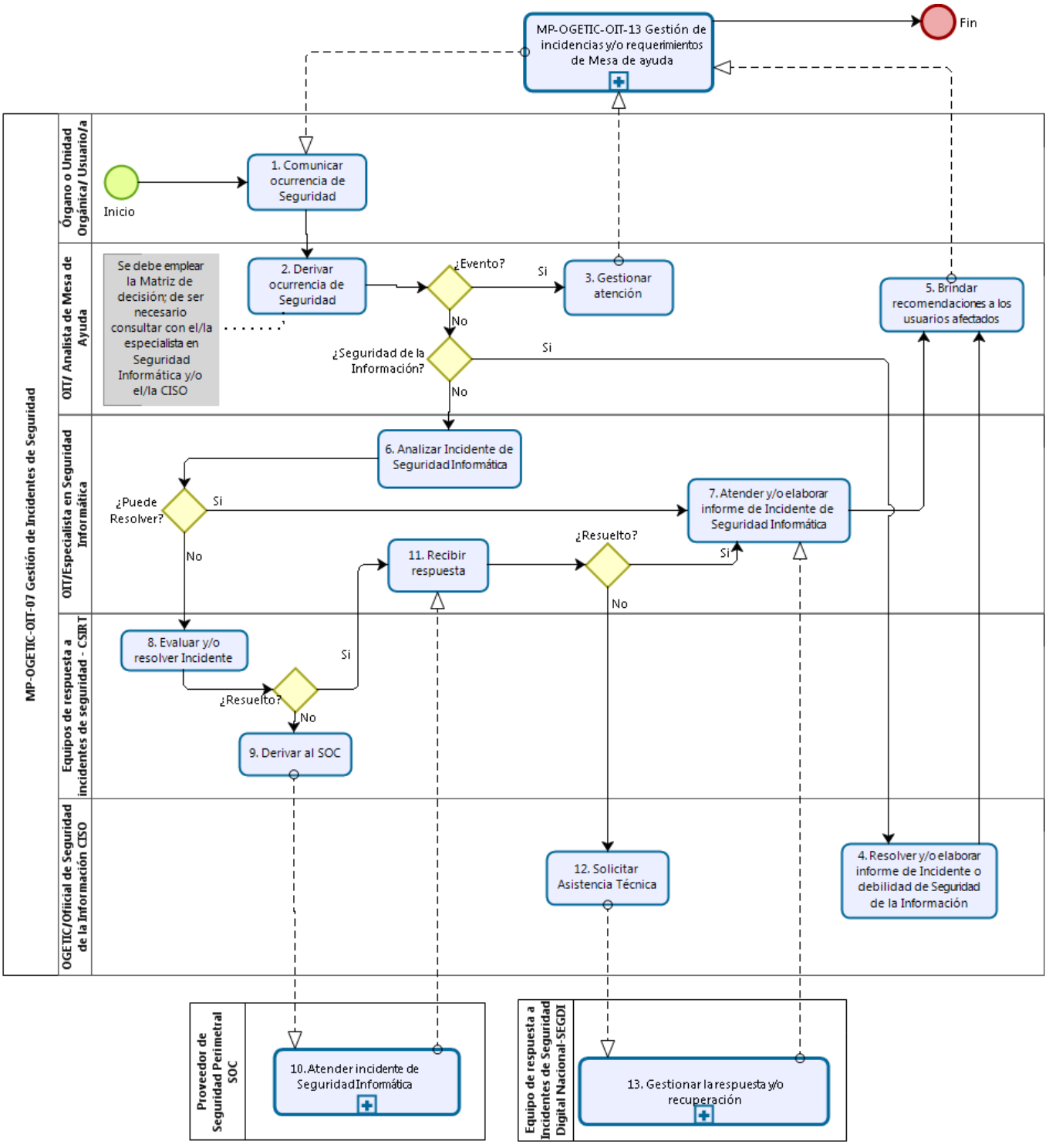
N° DE ACTIVIDAD	ÓRGANO O UNIDAD ORGÁNICA/ RESPONSABLE	ACCIÓN A SEGUIR
3	OIT/ Analista de Mesa de Ayuda	**Gestionar atención.-** Gestiona evento de seguridad conforme al MP-OGETIC-OIT-13 Gestión de incidencias y/o requerimientos de Mesa de ayuda.
4	OGETIC/ Oficial de Seguridad de la Información	**Atender y/o elaborar informe de incidente o debilidad de Seguridad de la Información.-** Analiza el impacto a la confidencialidad, integridad y disponibilidad ocasionado por el incidente/debilidad de seguridad de la información, lo atiende e informa de las acciones realizadas; considerando que dicho informe será empleado como base de conocimiento y aprendizaje para la solución de incidentes futuros. *Nota: A partir del análisis y la resolución de los incidentes de seguridad registrados en el sistema de mesa de ayuda, se remitirá de manera trimestral:* • *A la Oficina de Informática y Telecomunicaciones – OIT, un informe con la finalidad de reducir la probabilidad o el impacto de los incidentes en el futuro.* • *Al Comité de Gobierno Digital – CGD, un informe con las estadísticas de los incidentes de seguridad con la finalidad de ser considerado en la elaboración del informe anual que mide el progreso de la implementación del Sistema de Gestión de Seguridad de la Información (Resolución Ministerial N° 087-2019-PCM, literal f del artículo 2).*
5	OIT/ Analista de Mesa de Ayuda	**Brindar recomendaciones a los usuarios afectados.-** Recibe el informe de las acciones realizadas por parte del especialista en Seguridad Informática y/o Oficial de Seguridad de la Información, y emite las recomendaciones y/o lineamientos a seguir a los usuarios afectados. *Nota: En caso de producirse un incidente de seguridad y se requiera aplicar acciones disciplinarias, se gestionará la emisión de un informe por parte de la OGETIC al despacho de Secretaría General para la aplicación de las acciones que estime pertinente.*
6	OIT/ Especialista en Seguridad Informática	**Analizar Incidente de Seguridad Informática.-** Analizar y evaluar si se cuenta con facilidades técnicas para resolver el incidente. ¿Puede resolver incidente? Si: Continuar con el paso 8. No: Continuar con el paso 10.

N° DE ACTIVIDAD	ÓRGANO O UNIDAD ORGÁNICA/ RESPONSABLE	ACCIÓN A SEGUIR
7	OIT/ Especialista en Seguridad Informática	**Atender y/o elaborar informe de Incidente de Seguridad Informática.-** Ejecuta las acciones técnicas para resolver y/o mitigar el incidente y continúa en el paso 5.
8	OGETIC/ Equipo de Respuesta a Incidentes	**Evaluar y/o resolver Incidente.-** Evalúa y de tener las facilidades técnicas resuelve el incidente. ¿Se resuelve incidente? Si: Continua con el paso 11. No: Continua con el paso 9.
9	OIT/ Especialista en Seguridad Informática	**Derivar al SOC.-** Remite correo electrónico y/o registro de incidente en la plataforma tecnológica del SOC, y establece comunicación con el sectorista del proveedor de seguridad perimetral vigente, indicando los detalles del incidente de seguridad informática.
10	Proveedor de Seguridad Perimetral / SOC	**Atender incidente de Seguridad informática.-** Resuelve el incidente de Seguridad informática y comunica al Especialista en Seguridad Informática de la OIT.
11	OIT/ Especialista en Seguridad Informática	**Recibir respuesta.-** Recibe la comunicación del SOC con los resultados de las acciones técnicas realizadas. ¿Incidente resuelto? Si: Continuar en el paso 7. No: Continuar en el paso 12.
12	OGETIC/ Oficial de Seguridad de la Información	**Solicitar Asistencia Técnica.-** Enviar correo electrónico al Equipo de Respuesta a Incidentes de Seguridad Digital Nacional, indicando los detalles del incidente de seguridad informática y la recopilación de las acciones previas realizadas. *Nota: El Equipo de Respuesta a Incidentes de Seguridad Digital Nacional es responsable de Gestionar la respuesta y/o recuperación ante incidentes de seguridad digital en el ámbito nacional(literal i) del numeral 7.4 del artículo 7 del Decreto de Urgencia N° 007-2020).*
13	SEGDI/ Equipo de Respuesta a Incidentes de Seguridad Digital Nacional	**Gestionar la respuesta y/o Recuperación.-** Gestionar la respuesta y/o recuperación del incidente de seguridad informática. Continuar en el paso 7. **Fin del procedimiento**

5. Registros

- Ticket de solicitud del proveedor de seguridad perimetral.
- Correo electrónico de comunicación a los/las usuarios/as afectados/as.
- Correo electrónico de comunicación con la SEGDI.

6. Diagrama de flujo



7. Anexos

Anexo N° 01 – Matriz de Decisión de Incidentes de Seguridad

Si el suceso comunicado se encuentra dentro de la clasificación descrita a continuación, se convierte en un suceso de seguridad de la información. Considerar que la lista a continuación es una lista base que será actualizada por el/la Oficial de Seguridad de la Información; la cual deberá de tener la clasificación de eventos o incidentes de seguridad:

Categoría	Clasificación	Descripción
Hacking	Ataques de ingeniería social (phishing).	Recepción de correos electrónicos de remitentes desconocidos y/o páginas web de dudosa procedencia solicitando información personal. Ejemplo: *Correo electrónico de remitente desconocido y contenido dudoso, que incluye un enlace fraudulento donde solicitan "hacer clic" y registrar el correo electrónico y contraseña del usuario.*
	Ataque o infección por código malicioso.	Se refiere a la introducción de códigos maliciosos en la infraestructura tecnológica de la Entidad: Virus informáticos, troyanos, gusanos informáticos. Ejemplo: *Descarga de archivos adjuntos de dudosa procedencia, documentos creados como acceso directo, entre otros.*
Falla en las operaciones	No disponibilidad de servicios, red o comunicaciones.	Indisponibilidad del servicio de correo electrónico, red interna, servicio de internet, servicio de central telefónica, portales web, servicio de telefonía, sistemas de información, otros. Ejemplo: *Denegación de servicio, caída del sistema, pérdida de conectividad.*
	Fallas en los equipos del centro de datos.	Fallas en los equipos de respaldo, equipos de comunicaciones, aire acondicionado de precisión y otros equipos instalados en el centro de datos institucional. Ejemplo: *No funcionamiento del equipo de backup.*
Acceso a la información	Acceso a servicios tecnológicos no autorizados (acceso lógico)	Acceder a los equipos informáticos, a los sistemas de información, servicios web o red institucional sin contar con la autorización respectiva. Ejemplo: *Acceder remotamente a la red institucional, acceder a carpetas en red de otra Unidad Orgánica, contar con un perfil de internet no autorizado, entre otros.*
	Ingreso no autorizado a las instalaciones (acceso físico).	Ingreso de personal no autorizado al centro de datos institucional o las instalaciones de la OGETIC. Ejemplo: *Ingreso no autorizado de proveedores, personal de la OGETIC, vigilantes, personal del Ministerio*.
Custodia de la información	Divulgación no autorizada de la información.	Divulgación de información contenida en activos de información sin contar con la autorización respectiva. Ejemplo: *Correos electrónicos, bases de datos, sistemas de información.*
	Pérdida de información.	Pérdida de información en forma digital o física. Ejemplo: *Pérdida de información en los sistemas de información, correo electrónico, servidores, discos externos, carpetas en red, expedientes, otros.*
	Modificación no autorizada de la información.	Modificación de la información contenida en los sistemas de información, portales web sin contar con la autorización respectiva. Ejemplo: *SQL Injection, desfiguración de portales (defacement), otros.*

Categoría	Clasificación	Descripción
Cambios operaciones de los sistemas	Modificación o eliminación de sistemas sin no autorizado.	Instalación, modificación o eliminación en las reglas de negocio de los sistemas informáticos sin requerimiento o autorización del área usuaria. Ejemplo: *Implementación de reglas de negocio en un módulo sin acta de requerimiento.*
	Instalación de software no autorizado.	Instalación de software no autorizado. Ejemplo: *Instalación de software sin licencia de uso.*
Cumplimiento regulatorio	Incumplimiento de directivas o procedimientos institucionales.	Incumplimiento a las disposiciones legales emitidas por el Ministerio de Cultura. Ejemplo: *Incumplimiento a Directivas, incumplimiento al manual de procedimiento.*

7.1 Glosario de Términos:

- **Confidencialidad.-** Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas.
- **Disponibilidad.-** Propiedad de la información de ser accesible y utilizable por petición de una entidad autorizada.
- **Integridad.-** Propiedad de la información de ser exactita y completo.

7.2 Acrónimo

- **OIT.-** Oficina de Informática y Telecomunicaciones.
- **CISO.-** Oficial de Seguridad de la Información.
- **SOC.-** Centro de Operaciones de Seguridad.
- **SEGDI.-** Secretaría de Gobierno Digital.