PROCEDIMIENTO	Código: **S03.04.09.01**
	Versión: 01
	Vigencia: 24/09/2025
Dueño del proceso: Oficina de Administración	

GESTIÓN DE MONITOREO DE EVENTOS 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 14:56:05
	Víctor Chávez Gómez	Jefe de Tecnologías de la Información	Firmado digitalmente por: CHAVEZ GOMEZ Victor Hugo FAU 20380799643 soft Fecha: 23/09/2025 18:28:06
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 16:35:50
Aprobado por:	Alberto Blas Ortiz	Jefe de la Oficina de Administración	

Versión	Descripción de Cambios	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. **Acuerdo de nivel de servicio**: Identifica y define las necesidades del cliente, a la vez que controla sus expectativas de servicio en relación con la capacidad del proveedor.

2.1.2. **ANS**: Acuerdos de Niveles de Servicio.

2.1.3. **Condiciones inusuales de operación**: Resultados obtenidos frente a los estándares de diseño, acuerdos de niveles de servicio, acuerdos de nivel de operación u otras condiciones tecnológicas establecidas, con el propósito de mantener la confidencialidad, integridad y disponibilidad de los activos de información.

2.1.4. **Disponibilidad**: Es la capacidad de un servicio, componente o elemento de configuración para llevar a cabo su función cuando sea necesario.

2.1.5. **Elemento de configuración (CI):** Cualquier componente u otro activo del servicio que necesite ser gestionado con el objeto de proveer un servicio de TI.

Los CI pueden ser hardware, software, documentos y recursos.

2.1.6. **Evento**: Alerta o notificación creada por un servicio de TI, elemento de configuración o herramienta de monitorización. Los Eventos requieren normalmente que el personal de operaciones de TI tome acciones, y a menudo conllevan el registro de Incidentes.

2.1.7. **Evento Alerta**: Se asigna a aquellos eventos que indican que el servicio se aproxima a un umbral. Su objetivo es notificar a las personas, herramientas o procesos apropiados para que revisen la situación y tomen las medidas necesarias para evitar que se produzca una excepción.

2.1.8. **Evento excepción**: Se asigna a los eventos cuando indican que el servicio está operando de manera irregular: los ANS se han incumplido, etc. Las excepciones pueden representar un fallo total, un cese en una funcionalidad o una disminución del rendimiento. Sin embargo, no tienen por qué ser errores.

2.1.9. **Evento informativo:** Se asigna a aquellos eventos que no requieren, en principio, ninguna respuesta y que por tanto no representan una excepción.

2.1.10. **SIEM**: Es una herramienta de gestión de incidentes y eventos de seguridad, la cual tiene diferentes componentes como colectores, motor Correlacionador, aplicación de eventos e incidentes y bases de datos.

2.1.11. **TI**: Tecnologías de la Información

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.

3. RESPONSABILIDADES

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

3.1.1. Evaluar posibles tipos de evento que decanten en potenciales incidentes de seguridad de la información.
3.1.2. Registrar y comunicar atención de eventos
3.1.3. Registrar potenciales lecciones aprendidas sobre eventos de seguridad de la información evaluados

3.2. Del Especialista de tecnologías de información y redes

3.2.1. Apoyar en la Detección, Identificación y Resolución de eventos
3.2.2. Detectar, Identificar, Clasificar, Correlacionar y comunicar los eventos.
3.2.3. Elaborar de informe de evaluación de eventos

4. GENERALIDADES

Eventos.

Toda gestión de eventos es realizada por los especialistas de tecnologías de información y redes con soporte del OSCD

La gestión de monitoreo de eventos debe ejecutarse de con una disponibilidad de 7x24x365, durante la operación de la infraestructura, plataforma o servicios de TI.

Los eventos de tipo “potenciales incidentes de seguridad de la información” que hayan sido correlacionados y que el análisis correspondiente identifique como potenciales incidentes de seguridad, deberán ser gestionados como incidentes de seguridad de la información para una adecuada y oportuna atención.

Los especialistas de tecnologías de información y redes son responsables por la correcta ejecución de la operacional de gestión de eventos y es el único empoderado para realizar modificaciones al mismo.

Algunos eventos presentan situaciones que requieren que sean tratados a través de otras gestiones como incidentes, debido a su severidad, complejidad o impacto. El tratamiento o respuesta debe darse en términos de estas gestiones.

Los especialistas de tecnologías de información y redes realizan las actividades para madurar dicha gestión realizando las siguientes actividades:

- ✓ Informe mensual
- ✓ Aplicación de acciones de mejora
- ✓ Seguimiento a umbrales existentes
- ✓ Seguimiento a Backlog
- ✓ Levantamiento de información para servicios nuevos.

5. SECUENCIA DE ACTIVIDADES

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Analizar evento detectado			
1	Recolectar información de evento - Revisar notificaciones de eventos detectadas por las herramientas de monitoreo	Área de TI	Especialista de Tecnologías de Información y Redes
2	Identificar, Clasificar y Correlacionar Eventos - Se identifica el evento, se clasifica los eventos para definir qué tipo de afectación es, luego se correlacionan los eventos que notifiquen la misma causa para ser solucionado por parte de los responsables del servicio	Área de TI	Especialista de tecnologías de Información y Redes
3	Elaborar informe de evaluación de eventos	Área de TI	Especialista de Tecnologías de Información y Redes
Evaluar atención de evento			
4	Evaluar tipo de evento ¿Califica como incidente de seguridad de la información? Si: Ir a la tarea 05 No: Ir a la tarea 06	Área de TI	OSCD
Gestión de respuesta a incidentes de seguridad de la información			
5	Procedimiento de respuesta a incidentes de seguridad de la información	Área de TI	OSCD
Cierre de evento			
6	Registro de atención de evento - Se procede a registrar atención de evento y cerrar el evento reportado	Área de TI.	OSCD
7	Registro de lección aprendida - Registrar lección aprendida del evento detectado, para atención más oportuna de eventos similares futuros	Área de TI	OSCD
8	Comunicar atención de evento	Área de TI	OSCD
Fin			

6. ANEXOS (Opcional)

6.1. Anexo 1 - Flujograma de procedimiento de gestión de monitoreo de eventos de seguridad de la información

Anexo N° 01

Flujograma de procedimiento de gestión de monitoreo de eventos de seguridad de la información