| Osinergmin<br>Organismo Supervisor de la Inversión en Energía y Minería | **PROCEDIMIENTO ESPECIFICO**<br><br>**"GESTIÓN DE ACTIVOS DE INFORMACIÓN"** | **Código : PE22-PE-04**<br>**Revisión : 02**<br><br>**Página : 1 de 12** |
|---|---|---|
| **Código y Nombre del Proceso** | PE22: Gestión por Procesos | |

| **Elaborado por:** | **Revisado por:** |
|---|---|
| Carlos Gonzales Fung<br>Oficial de Seguridad de la Información | Isaac Maguiña Soriano<br>Especialista Senior de Procesos y Sistemas de Gestión |

**Aprobado por:**

Julio Lazo Abadie
Gerente Planeamiento, Presupuesto y Modernización

Firmado Digitalmente
por: LAZO ABADIE
Julio Alfonso Leonidas
FAU 20376082114 hard
Fecha: 25/02/2020
19:12:00

## 1. OBJETIVO:

Realizar una adecuada gestión de los activos de información de la organización, de manera que se asegure el cumplimiento de requisitos de seguridad de información y cumplimiento normativo.

## 2. ALCANCE:

El presente procedimiento tiene alcance a toda la organización y puede ser parte del proceso de Gestión de Riesgos de Seguridad de Información. Comprende la identificación, inventario, clasificación, valoración, etiquetado y uso adecuado de los activos de información.

## 3. BASE NORMATIVA:

a. Norma ISO 27001:2013

## 4. SIGLAS Y DEFINICIONES:

| Rubro | Descripción |
|---|---|
| a. Activo de información | Es todo aquel que contiene información y tiene valor a los procesos de Osinergmin, siendo necesarios para asegurar la continuidad y buen desempeño de los procesos |
| b. SI | Seguridad de la información |
| c. Incidente de seguridad de la información (ISI) | Uno o muchos eventos inesperados o no deseados, que tienen una probabilidad significativa de comprometer la disponibilidad, confidencialidad e integridad de los principales activos de la información de los procesos de OSINERGMIN y de amenazar la seguridad de la información. |
| d. SE | Secretaria Ejecutiva |
| e. SGI | Sistema de gestión de seguridad de la información |
| f. Vulnerabilidad | Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza. |
| g. Vulnerabilidad de seguridad de la Información (VSI) | Debilidad de un activo o grupo de activos de información que puede ser explotada potencialmente por una o más amenazas, comprometiendo su disponibilidad, confidencialidad e integridad. |

## 5. REQUISITOS PARA INICIAR EL PROCEDIMIENTO:

| Descripción | Fuente |
|---|---|
| Realización de la Gestión de Riesgos de Seguridad de Información | Instructivo "Gestión de Riesgo de SI" I4-PE2-2-PE-02 |
| Solicitud de identificación, inventario, clasificación, valoración, etiquetado y uso adecuado de los activos de información | Solicitud remitida por memorándum o correo. |

## 6. ACTIVIDADES: se adjunta diagrama de flujo, **Anexo.1**

| Entradas/quien lo brinda | ACTIVIDAD (del diagrama Anexo.1) | Descripción (Responsables, que se hace, cómo se hace, plazos) | Resultados (Salidas/Registros) | Destinatarios |
|---|---|---|---|---|
| • Gestión de Riesgos de Seguridad de Información<br>• Solicitud para la Gestión de Activos de Información | **1. Elaboración Inventario de Activos** | El Responsable del Proceso, con apoyo del Coordinador SIG del área registran los activos de información en el formato "**Inventario de Activos de Información, F1-PE22-PE-04"** según lo siguiente:<br>a. Asigna el código y nombre al activo de información.<br>b. Establece la categoría del activo: Los activos son categorizados y registrados según las categorías descritas en el **Anexo.4.**<br>c. Describe al activo de información, conceptualizándolo dentro del proceso funcional, | Inventario de activos de información | • Coordinador institucional<br>• Propietario de Activo de Información<br>• Coordinador SIG<br>• Responsable de procesos |

| Entradas/quien lo brinda | ACTIVIDAD (del diagrama Anexo.1) | Descripción (Responsables, que se hace, cómo se hace, plazos) | Resultados (Salidas/Registros) | Destinatarios |
|---|---|---|---|---|
| | | sus características (documentación en papel, software, hardware), y sus requerimientos respecto de seguridad de la información.<br>d. Registra la ubicación física o lógica del activo. En el caso de ubicación física, detallar la instalación donde se encuentra y si la gestión es tercerizada o propia. En el caso del activo lógico detallar el nombre del archivo de la base de datos o esquema y del servidor donde se encuentra, si se encuentra en redundancia y/o respaldo.<br>e. Identifica al ***responsable y custodio del activo de información***, teniendo en cuenta lo siguiente:<br>✓**Propietario del activo:** Registrar el cargo y área del responsable de controlar la producción, desarrollo, mantenimiento, uso y seguridad del activo de información. Tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo.<br>✓**Custodio del activo:** Registrar el cargo y área del responsable que opera, emplea, mantiene y protege al activo de información como parte de sus funciones regulares. Puede haber más de un custodio.<br>f. Identifica y señalar si el activo de información se encuentra asociado a exigencias legales, reglamentarias o contractuales.<br>g. Registra el tipo de activo según la categoría a la que corresponde y conforme al **Anexo.5.**<br>h. Clasifica el activo de información según lo especificado en el punto 2. ***Clasificación y Tratamiento del activo***.<br>i. Valora el activo de información según lo especificado en el punto 3. ***Valorización del activo***.<br>j. Gestiona la aprobación del inventario de Activos de Información por el Responsable del Proceso, Coordinador SIG del área y el Propietario de Activos de Información. | | |
| Inventario de activos de información | **2. Clasificación y Tratamiento del activo** | a. Los propietarios clasifican los activos de información considerando su nivel de uso y autorización de acceso, teniendo en consideración el **Anexo.6**.<br>b. Los custodios de información cumplen las medidas de tratamiento especificadas en la Tabla 3. según la clasificación de los activos de información que custodian. | Inventario de activos de información | • Coordinador institucional<br>• Propietario de Activo de Información<br>• Coordinador SIG<br>• Responsable de procesos |
| Inventario de activos de información | **3. Valorización del activo** | a. Se estima el valor del activo de información, teniendo en cuenta su importancia sobre el desempeño y continuidad del proceso, y respecto de sus requerimientos de confidencialidad, integridad y disponibilidad, calculándose como el promedio de los valores asignados a cada atributo, especificados en el **Anexo.7.**<br>b. Se estima la tasación del activo de información, identificando el valor del activo dentro del rango de tasación, bajo los criterios detallados en el **Anexo.7.** | Inventario de activos de información | • Propietario de Activo de Información<br>• Coordinador institucional<br>• Coordinador SIG<br>• Responsable de procesos |

| Entradas/quien lo brinda | ACTIVIDAD (del diagrama Anexo.1) | Descripción (Responsables, que se hace, cómo se hace, plazos) | Resultados (Salidas/Registros) | Destinatarios |
|---|---|---|---|---|
| Inventario de activos de información | **4. Etiquetado del activo** | a. El propietario del activo vela por la adecuada aplicación del etiquetado de sus activos, ya sean de carácter confidencial y restringido, y según los siguientes criterios:<br>**Documentación física:** Para la información que se clasifica como confidencial o restringida el etiquetado se establece por el propietario de información.<br>**Documentos digitales:** Para la información que se clasifica como confidencial o restringida el etiquetado se establece por el propietario de información.<br>**Correo electrónico:** Todo correo electrónico generado por los miembros de la organización estará sujeto a una declaratoria de confidencialidad que hace explícito el carácter reservado de todo correo electrónico. El contenido del etiquetado del correo electrónico se presenta en el siguiente cuadro:<br>"El sistema de correo de Osinergmin ésta destinado únicamente para fines informativos y/o laborales, cualquier otro uso contraviene las políticas de la Institución. Toda información contenida en este mensaje es confidencial y de uso exclusivo de Osinergmin. Su divulgación, copia y/o adulteración están prohibidas y sólo debe ser conocida por la persona a quien se dirige este mensaje. Si usted ha recibido este mensaje por error por favor proceda a eliminarlo y notificar al remitente."<br>**Base de datos:** La documentación de análisis y arquitectura de las bases de datos de la organización indica de forma explícita cuáles son aquellas tablas o componentes de la misma tienen una clasificación confidencial o restringida.<br>**Software de sistema:** La documentación de análisis y arquitectura de los sistemas desarrollados o adquiridos por la organización indica de forma explícita cuáles son aquellos módulos o componentes de la misma tienen una clasificación confidencial o restringida.<br>**Activos físicos:** Para la información que se clasifica como confidencial o restringida el etiquetado se establece por el propietario de información. | Etiquetado del activo de información | • Propietario de Activo de Información<br>• Coordinador institucional<br>• Coordinador SIG<br>• Responsable de procesos |
| Inventario de activos de información | **5. Uso Adecuado del activo** | El propietario de los activos de información establece, registra, aprueba y difunde el uso aceptable y no aceptable de los activos de información. Para ello usa el modelo establecido en el **Anexo.8** ***"Uso Aceptable de Activos de Información"***. La difusión se hace a través de la WEB del SIG. | Uso Aceptable de activo de información | • Propietario de Activo de Información<br>• Coordinador institucional<br>• Coordinador SIG<br>• Responsable de procesos |

## 7. ANEXOS:

a. Anexo.1: Diagrama de flujo
b. Anexo.2: Ficha Resumen del procedimiento específico
c. Anexo.3. Ficha de indicador de desempeño
d. Anexo.4: Categoría de activos de información
e. Anexo.5: Tipo de activos de información

f. Anexo.6: Clasificación del activo de información
g. Anexo.7: Valor del activo de información
h. Anexo.8: Modelo del Uso aceptable del activo de información

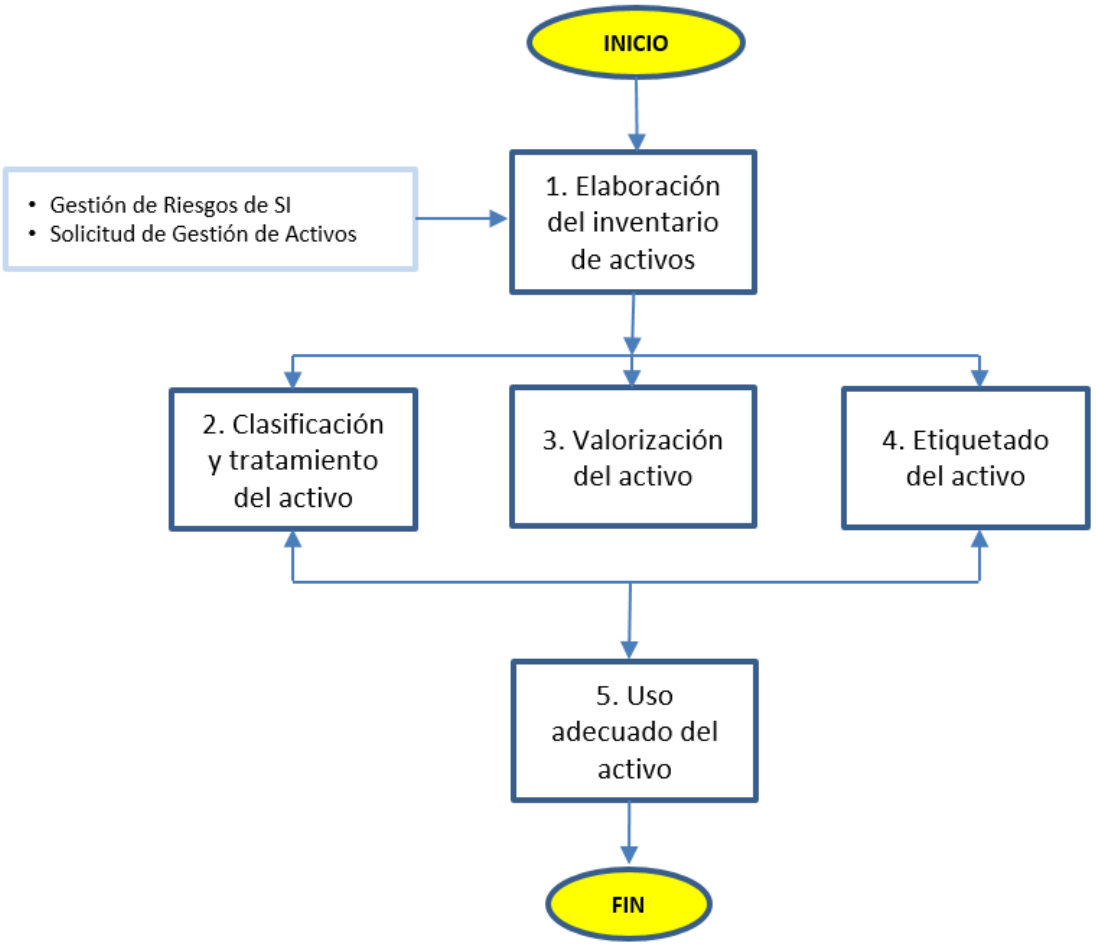
## 8. REGISTROS:

a. Inventario de Activos de Información, F1-PE2-2-PE-04
b. Uso Aceptable del activo de información

## 9. CONTROL DE CAMBIOS:

| Numeral/otros | Descripción del cambio | Descripción del sustento |
|---|---|---|
| **Actualización de código del procedimiento** | **De PE2-2-PE-04 a PE22-PE-04** | Actualización conforme a la NT N° 001-2018-PCM/SGP "Implementación de la Gestión por Procesos en las Entidades de la Administración Pública" aprobado por Resolución de secretaría de Gestión Pública N° 006-2018-PCM/SGP. |
| **Título** | Cambio de nombre de "Valorización de Activos de Información" a "Gestión de Activos de Información" | El procedimiento no solo consiste en valorizar, sino en varias actividades que comprenden la Gestión de Activos de Información. |
| **1. Objetivo y 2. Alcance** | Adecuaciones | Precisiones en cuanto al objetivo y alcance del procedimiento. |
| **5. Requisitos para iniciar procedimiento** | Se indicó las actividades que disparan este procedimiento. | Versión Inicial |
| **6. Actividades** | Se indicó las salidas correctas en las actividades 4 y 5 | Correcciones. |
| **Anexo 3. Ficha de Indicador** | Se definió indicador | Versión inicial. |
| **Anexo 6. Clasificación de Activos de Información** | Se precisó el caso de "Uso Interno" | Precisiones en cuanto a que la información es de uso de la organización. Esto producto de una observación de auditoría. |

**ANEXO.1: Diagrama de Flujo del Procedimiento Específico**



## ANEXO.2 Ficha Resumen del Procedimiento Específico

| | |
|---|---|
| **Responsable del PE** | **Especialista Senior de Procesos** |

| Actividad | Responsable (puesto) | Registros | Plazos (días hábiles) |
|---|---|---|---|
| **1. Elaboración del inventario de activos** | 1. Coordinador institucional SGI<br>2. Coordinador SIG<br>3. Responsable de procesos<br>4. Propietario de Activo de Información | 1. Inventario de activos de información<br>2. Uso aceptable del activo de información | - |
| **2. Clasificación y tratamiento del activo** | | | |
| **3. Valorización del activo** | | | |
| **4. Etiquetado del activo** | | | |
| **5. Uso adecuado del activo** | | | |
| | | **Plazo Total del PE** | - |

## ANEXO.3: Ficha de indicador de desempeño

| | |
|---|---|
| **1. Nombre del Proceso** | PE22-PE-04 Valorización de Activos de Información |
| **2. Objetivo del Proceso** | Realizar una adecuada gestión de los activos de información de la organización, de manera que se asegure el cumplimiento de requisitos de seguridad de información y cumplimiento normativo. |

| | |
|---|---|
| **3. Nombre del Indicador** | **% Cumplimiento de registro de activos de información** |
| **4. Finalidad del indicador** | Asegurar que los activos de información estén identificados y gestionados. |
| **5. Fórmula** | (N° registros de inventario de activos de información por proceso actualizados por año / N° procesos de la organización) x 100 |
| **6. Unidad de medida** | Porcentaje |
| **7. Frecuencia** | Trimestral |
| **8. Oportunidad de medida** | Anual |
| **9. Línea base** | No Aplica |
| **10. Meta** | 100% |
| **11. Fuente de datos** | Formato F1- PE22-PE-04 |
| **12. Responsable** | Coordinador institucional SGI |

## Anexo.4

## CATEGORÍA DE ACTIVOS DE INFORMACIÓN

| Tipos | Categorías | Descripción |
|---|---|---|
| **Activos de Información Documental / Digital** | Información escrita | Documentos creados y/o conservados en papel (planes, programas, estudios, informes, material de entrenamiento, contratos firmados, reportes, certificados, facturas, memos, documentos de embarque, etc.) |
| | Información electrónica | Base de datos y documentos creados y o conservados en medios electrónicos (correo electrónico, audio, video, cintas, dvd, entre otros). |
| | Información hablada | Conversaciones presenciales, telefónicas, presentaciones orales o a través de medios virtuales (video conferencia). |
| **Activos de software** | Software base o sistema operativo | Windows, Linux, etc. |
| | Software comercial o herramientas, utilitarios | Office, Adobe, Exchange, entre otros. |
| | Software desarrollado por terceros | SAP, PEOPLE SOFT, ORACLE, JD EDWARDS, etc. |
| **Activos de software** | Software desarrollado internamente | Sistema Integrado, Aplicativo, Sistema de Información. |
| | Software de administración de Base de Datos | SQL, ORACLE, DB/2, INFORMIX, MYSQL, entre otros |
| | Otro Software | Software específicos desarrollados por terceros. |
| | Equipo de procesamiento | Servidores, computadoras, laptops, entre otros. |
| | Equipo de comunicaciones | Red LAN (ruteadores, switches), red telefonía (central teléfonos), red inalámbrica (Access point), entre otros. |
| | Medio de almacenamiento | Discos, cintas, disquetes, CD's, DVD's, memorias USB, entre otros. |
| | Mobiliario y Equipamiento | Cajas Fuertes, Estantes, gavetas, etc. |
| | Otros equipos | - |
| **Servicios (Terceros)** | Procesamiento y comunicaciones | Outsourcing TI, de procesamiento de la información, de impresión, de fotocopiado, de mensajería, de internet, telefonía fija y celular, entre otros. |
| | Servicios generales | Energía eléctrica, abastecimiento de agua, suministro de gas, calefacción, aire acondicionado, entre otros. |
| | Otros servicios | Servicio de intermediación laboral, proveedores de servicios (externos), entre otros. |
| **Recurso Humano** | Clientes | Usuarios y consumidores de los servicios de la Institución. |
| | Personal | Personal contratado directamente por OSINERGMIN bajo las modalidades de Planilla, Contratación Administrativa de Servicios, Pasantes y practicantes. |
| | Directores | Miembros del Consejo Directivo. |
| | Personal Externo | Personal externo contratado por proyecto o actividad específica que tiene un inicio y fin definido. |

## Anexo.5

## TIPO DE ACTIVO DE INFORMACIÓN

| Categoría | Tipo |
|---|---|
| **Información Documental** | Información electrónica |
| | Información escrita |
| | Información hablada |
| **Software** | Software base o sistema operativo |
| | Software comercial o herramientas, utilitarios |
| | Software desarrollado por terceros |
| | Software desarrollado internamente |
| **Software** | Software de administración de Base de Datos |
| | Otro Software |
| **Activo Físico** | Equipo de procesamiento |
| | Equipo de comunicaciones |
| | Medio de almacenamiento |
| | Mobiliario y Equipamiento |
| | Otros equipos |
| **Servicios de Terceros** | Procesamiento y Comunicaciones |
| | Servicios Generales |
| | Otros Servicios |
| **Personal** | Clientes |
| | Personal |
| | Directores |
| | Personal Externo |

## Anexo.6

## CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN

| Clasificación | Descripción | Tratamiento |
|---|---|---|
| **Público** | Información explícitamente aprobada para su diseminación pública. Los ejemplos incluyen, boletines de noticias, comunicados internos, presupuestos, memorandos, informes de prensa, entre otros. | **Transporte:** Mediante cualquier medio<br>**Almacenamiento:** Usualmente esta información es transitoria, por lo tanto se almacena una copia controlada dentro de la organización, por cualquier medio, y copias no controladas cuando salga del ámbito de control de la institución. |
| **Interno** | Se espera que la revelación de esta información no cause daños serios a Osinergmin, y su acceso es solo para los empleados de la entidad a través de la intranet, servidores de archivos u otros medios de almacenamiento, publicación y acceso. El acceso a la información es de acuerdo con sus funciones.<br>Los ejemplos pueden ser información personal o reportes realizados por un área específica o las bases de datos provistas por entidades externas que requieren primero ser procesadas antes de su publicación.<br><br>Esta es la clasificación por defecto para la información que no tiene una designación específica. | **Transporte:** Por cualquier medio que forme parte de la infraestructura tecnológica INTERNA y por los custodios de dicha información.<br><br>**Almacenamiento:** Sólo tienen acceso los explícitamente autorizados. Se mantiene dentro de los confines de la Organización, física o lógicamente. |
| **Confidencial** | El acceso a esta información es estrictamente restringido basándose en el concepto de "necesidad de saber". La revelación de esta información requiere la aprobación de su propietario o del grupo al cual pertenece este y es de uso exclusivo interno de la organización y en el caso de terceros, el acuerdo de confidencialidad firmado. La confidencialidad prohíbe la divulgación no autorizada de la información. | Esta es manejada con todas las precauciones y controles posibles determinando exactamente que personas tienen acceso a la misma y vigilando su uso, transporte y almacenamiento. Cada copia debe tener un código de reproducción y llevar impreso el nombre del destinatario, además del rótulo "copia no controlada" cuando sale del ámbito de los controles institucionales.<br><br>**Transporte:** Por medios seguros, encriptados y siempre utilizando acuses de recibo. Debe ser realizado, preferiblemente, por los propietarios y/o custodios de la información.<br><br>**Almacenamiento:** Se mantiene cifrada en un medio protegido con controles de acceso físico o lógico, y de ser el caso bajo llave u otro mecanismo de protección (acceso sólo al dueño o propietario). |

| Clasificación | Descripción | Tratamiento |
|---|---|---|
| **Restringido** | El acceso a esta información se da a un número reducido de personas, una o dos, de alcanzar el privilegio a más personas se debe justificar las razones. Usualmente, debe ir acompañada del principio de confidencialidad. | Esta debe ser manejada con todas las precauciones y controles posibles determinando exactamente qué personas tienen acceso a la misma y vigilando su uso, transporte y almacenamiento. Cada copia debe tener un código de reproducción y llevar impreso el nombre del destinatario, además del rótulo "copia no controlada" cuando sale del ámbito de los controles institucionales.<br><br>**Transporte:** Por medios seguros, encriptados y siempre utilizando acuses de recibo. Debe ser realizado por los custodios de la información.<br><br>**Almacenamiento:** Se mantiene cifrada en un medio protegido con controles de acceso físico o lógico, y de ser el caso bajo llave u otro mecanismo de protección (acceso sólo al dueño o propietario). |