PROCEDIMIENTO	Código: **S03.04.09.02**
	Versión: 01
	Vigencia: 24/09/2025
Dueño del proceso: Oficina de Administración	

GESTIÓN DE CAPACIDAD DE LA PLATAFORMA TÉCNOLOGICA

	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 14:55:13
	Víctor Chávez Gómez	Jefe de Tecnologías de la Información	Firmado digitalmente por: CHAVEZ GOMEZ Victor Hugo FAU 20380799643 soft Fecha: 23/09/2025 18:29:54
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 16:36:19
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. **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. **Análisis de tendencia:** Método utilizado para identificar patrones y direcciones en datos a lo largo del tiempo, con el objetivo de predecir comportamientos futuros o comprender mejor la situación actual

2.1.3. **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.

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

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

2.1.6. **Escalabilidad:** Capacidad de un sistema, red o proceso para manejar una cantidad creciente de trabajo de manera eficiente y elegante, sin comprometer su rendimiento ni funcionalidad

2.1.7. **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”.

2.1.8. **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.

2.1.9. **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.

2.1.10. **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.

2.1.11. **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.

2.1.12. **Monitoreo:** Proceso continuo de observar y seguir de cerca el progreso de un proyecto, programa, o actividad con el fin de evaluar su desempeño y detectar posibles problemas o desviaciones con respecto a los objetivos planteados

2.1.13. **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.

2.1.14. **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.

2.1.15. **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.

3. RESPONSABILIDADES

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

3.1.1. Supervisar el cumplimiento de monitoreo de la plataforma tecnológica de la entidad.

3.1.2. Realizar coordinaciones con el Equipo de tecnología de información para la atención de desviaciones en la capacidad de almacenamiento o procesamiento de la plataforma tecnológica de la institución.

3.1.3. Implementar y mantener controles de seguridad de la información que puedan responder de manera efectiva a la necesidad de mantener la capacidad de almacenamiento y procesamiento de la plataforma tecnológica.

3.1.4. Planificar y realizar la revisión de cumplimiento de controles.

3.2. Del jefe de TI

3.2.1. Revisar y aprobar los planes de mejora producto de los resultados de informe de capacidad.

3.3. Del Especialista de tecnologías de información y redes

3.3.1. Monitorear y planificar la capacidad de la plataforma tecnológica.

3.3.2. Proponer alternativas de solución a incidentes asociadas a la capacidad de la plataforma tecnológica.

3.3.3. Informar al OSCD y alta dirección mejoras a la capacidad de almacenamiento y procesamiento de la plataforma tecnológica.

4. GENERALIDADES

4.1. Asegurar que los recursos de TI (hardware, software, redes y personal) sean adecuados para cumplir con los requisitos de seguridad de la información y mantener la disponibilidad, integridad y confidencialidad de los datos.

- Es responsabilidad del OSCD y del Área de TI, efectuar el monitoreo de la necesidad de capacidad en recursos y de los sistemas en operación que soportan el proceso de Gestión de portafolio de proyectos de PROINVERSION y proyectar las necesidades futuras, a fin de garantizar un procesamiento y almacenamiento adecuados. Se tendrá en cuenta además los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información para el periodo estipulado de vida útil de cada componente.
- Es responsabilidad del Área de TI informar las necesidades detectadas por su personal a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una acción correctiva adecuada.
- Es responsabilidad del Área de TI informar el rendimiento de las diferentes plataformas de servidores, almacenamiento, infraestructura, conectividad y detección de posibles fallas que amenacen la continuidad del procesamiento.
- El Área de TI debe presentar informe y plan de reingeniería de capacidad a las autoridades competentes para su aprobación. Asimismo, el OSCD podría coordinar o realizar auditorías internas para su verificación.
- El equipo de TI recibirá y evaluará el Reporte de Niveles de Capacidad emitido para las atenciones correspondientes.

4.2. Planificación de capacidad de las redes de comunicaciones

- El Área de TI con apoyo del OSCD analizará el uso de las redes de comunicaciones con el objetivo de ajustar y planificar la capacidad de las líneas y los elementos de red (routers, switches, etc.) de acuerdo con el rendimiento esperado y así evitar posibles fallos, de requerirse o aplicar.
- Estas planificaciones deben tener en cuenta los requisitos de tiempo de respuesta en el acceso a la información y los sistemas que la tratan, así como la tendencia actual proyectada del acceso a los recursos.
- Asimismo, se planificará la red para que responda automáticamente a los cortes en las líneas o fallos de los dispositivos esenciales de encaminamiento y equipamiento de la red (líneas de backup, redundancia, etc.).

4.3. Planificación de la capacidad de la plataforma de servidores y almacenamiento

- El Área de TI con apoyo del OSCD analizará el uso de los servidores, bases de datos y los dispositivos de almacenamiento con el objetivo de ajustar y realizar una planificación (consumo de CPU, crecimiento del espacio en disco utilizado, consumo de memoria, etc.) de acuerdo con el rendimiento esperado y así evitar posibles fallos, para ello podrá considerarse configuraciones automáticas de autoajuste.

4.4. Planificación de capacidad de recurso humano

- El Área de TI con apoyo del OSCD, analizaran la suficiencia de capacidad de recurso humano para la atención de los servicios tecnológicos que dan soporte al proceso de Gestión de portafolio de proyectos.

4.5. Acciones para el aumento de capacidad

- Evaluar la incorporación de personal de apoyo temporal, cuando se evidencie que por la cantidad y carga de proyectos se necesite.
- Evaluar ampliar el centro de procesamiento de información, si el espacio físico ya resulta no suficiente.
- Evaluar eliminación de datos obsoletos en bases de datos de ya no ser requeridos o relevantes por los usuarios.
- Eliminación de registros impresos que hayan cumplido su período de retención (liberar espacio en oficinas).
- Optimizar el código de la aplicación o las consultas a la base de datos.

- Negar o restringir el ancho de banda para los servicios que consumen recursos si estos no son críticos (por ejemplo, transmisión de video).

5. SECUENCIA DE ACTIVIDADES

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Programar evaluación de capacidad			
1	Seleccionar activos a los cuales se les medirá la capacidad	Área de TI	OSCD
2	Elaborar programa de evaluación de capacidad sobre los activos seleccionados (Infraestructura, redes, recurso humano, etc.)	Área de TI	OSCD
Coordinar evaluación de capacidad			
3	Asignar evaluación de capacidad a especialista	Área de TI.	OSCD
Ejecutar prueba de capacidad a plataforma			
4	Evaluar capacidad de plataforma tecnológica • Realizar proyecciones basadas en datos históricos. • Identificar posibles cuellos de botella. • Planificar actualizaciones o mejoras antes de alcanzar límites críticos. Evaluar: • Uso actual vs. capacidad máxima. • Proyecciones de crecimiento (ej.: 6–12 meses). • Riesgos de saturación	Área de TI.	Especialista de Tecnologías de Información y Redes
5	Preparar informe de capacidad de plataforma tecnológica	Área de TI.	Especialista de Tecnologías de Información y Redes
Preparar plan de mejora a la capacidad de la plataforma			
6	Analizar si se recomienda plan de mejora a la capacidad ¿Requiere plan de mejora de capacidad? Si: Ir a la tarea 7 No: Ir a la tarea 8	Área de TI.	Especialista de Tecnologías de Información y Redes
7	Elaborar plan de mejora de capacidad	Área de TI.	Especialista de Tecnologías de Información y Redes
Revisar aprobación de plan de mejora			
8	Revisar plan de mejora de capacidad ¿Se aprueba plan de mejora de capacidad? Si: Ir a tarea 9 No: Ir a tarea 7	Área de TI.	Jefe de TI
9	**Aprobación de plan de mejora** Revisión y aprobación de plan de mejora recomendado	Área de TI.	Jefe de TI
Documentar ejecución de plan de mejora			
10	Registrar plan de mejora La documentación se debe resguardar y archivar desde el análisis de capacidad • Informes de capacidad. • Evidencias de pruebas de rendimiento. • Aprobaciones de la gerencia (Decisiones de mejora) • Plan de mejora recomendado	Área de TI.	OSCD
11	Programar ejecución de plan de mejora de capacidad	Área de TI.	OSCD
Fin			

6. ANEXOS (Opcional)

6.1. Plan de capacidad

6.2. Diagrama de flujo de procedimiento de gestión de capacidad de la plataforma tecnológica

Anexo N° 01

Plan de capacidad

Para el desarrollo de plan de capacidad se debe de considerar los siguientes lineamientos:

Estrategia de medición

Para plan de capacidad se ha determinado efectuar la medición de los niveles de utilización de algunos activos de la plataforma tecnológica, entre los cuales se encuentran:

- Servicio de respaldo (backup)
- Servidor de Aplicación (Espacio en disco, memoria, procesamiento)
- Base de datos (Espacio en disco, memoria, procesamiento)
- Capacidad de recurso humano para la atención de proyectos

Esto con el objetivo de asegurar que se cuente con la disponibilidad suficiente de recursos y que se realicen las provisiones necesarias para evitar sobre carga de utilización que afecte la normal operativa del servicio provisto por el área de TI

Medición de indicadores

Se han establecido indicadores para cada activo de información requerido que da soporte al alcance del SGSI, así como umbrales de procesamiento, con el objetivo de anticipar una ventana de tiempo suficiente antes de que se sature el activo tecnológico.

Esto permitirá a la Jefatura de TI realizar una eficiente toma de decisiones.

Se llevará un control de medición con periodicidad mensual, durante 1 año, renovable de acuerdo con la necesidad

Backup:

Valor: Espacio en disco para almacenamiento:
Frecuencia de medición: Mensual
Umbral objetivo: 80%

Servidores:

Valor: Porcentaje de procesamiento, memoria y almacenamiento
Frecuencia de medición: Mensual
Umbral objetivo: 75%, 75% y 80%

Formato de medición

Se utilizará un formato de gestión de capacidad, con el objetivo de recopilar la información de los valores de medición y poder monitorear el nivel de dimensionamiento y capacidad de los activos críticos de la organización y poder tomar acciones oportunas en harás de asegurar su continuidad y correcto procesamiento

Desarrollo o planificación de proyectos tecnológicos durante el presente año, que afecten la capacidad instalada de la organización

Se debe incluir en el plan de capacidad, si producto de los proyectos aprobados para el presente año se podrá afectar la capacidad para la atención de los servicios de TI, y desarrollar las acciones a ejecutar en caso se evidencia necesidad de incrementar la capacidad

Anexo N° 02 - Flujograma de gestión de la capacidad de la plataforma tecnológica