PROCEDIMIENTO	Código: **S03.04.12**
	Versión: 01
	Vigencia:24/09/2025
Dueño del proceso: Oficina de Administración	

SEGURIDAD DE CONECTIVIDAD DE LA RED INTERNA Y SERVICIOS DE RED

	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 14:43:34
	Víctor Chávez Gómez	Jefe de Tecnologías de la Información	Firmado digitalmente por: CHAVEZ GOMEZ Victor Hugo FAU 20380799643 soft Fecha: 23/09/2025 18:35:10
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 16:38:40
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, y/o
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. **Firewall:** Dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente.

2.1.2. **Antivirus:** Software utilizado para evitar, analizar, detectar y eliminar virus de los dispositivos.

2.1.3. **LAN:** Local Área Network, son un conjunto de dispositivos conectados entre sí que comparte comunicación o enlaces con un servidor

2.1.4. **WAN**: Wide Área Network, consiste en varias redes locales unidad, aunque su ubicación física no sea la misma

2.1.5. **Autenticidad**: Propiedad que tiene una entidad de ser genuina y de poder demostrar que es realmente quien o lo que afirma ser.

2.1.6. **Confidencialidad**: Principio de la seguridad de la información que busca asegurar que solo quienes estén autorizados puedan acceder a la información

2.1.7. **Integridad**: Principio de la seguridad de la información que busca asegurar que la información y sus métodos sean exactos y completos.

2.1.8. **No repudio**: Capacidad para demostrar la ocurrencia de un evento o acción reclamada y sus entidades de origen.

2.1.9. **Log**: Es el registro de los eventos y acciones sucedidas

2.1.10. **P2P**: Es una red de ordenadores en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

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 Especialista de tecnologías de información y redes

3.1.1. Administrar, gestionar y velar por la seguridad de los equipos conectados a la red de PROINVERSION.

3.1.2. Supervisar y participar de la instalación y mantenimiento de la red.

3.1.3. Determinar las necesidades de utilización de los servicios de red y los accesos de los usuarios a la red.

3.1.4. Administrar las redes.

3.1.5. Monitorear los servicios de red.

3.1.6. Identificar, diagnosticar y resolver fallos que se presenten en la red.

3.1.7. Identificar, evaluar y proponer mejoras en el uso de la red

3.2. Del Jefe de TI

3.2.1. Desarrollar el proceso de Seguridad de las Comunicaciones cumpliendo los plazos y las disposiciones previstas en la normativa legal y el presente procedimiento.

3.2.2. Garantizar la protección de los recursos de las redes de comunicación, entre los que se consideran:

- Recursos de comunicación como redes LAN, canales dedicados de datos, entre otros.
- Recursos hardware y software.
- Servicios de comunicación

3.2.3. Evaluar y autorizar las mejoras a implementarse en la red y sus servicios de red

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

3.3.1. Evaluar y desarrollar propuesta de mejoras en los controles de seguridad sobre la red

3.3.2. Documentar toda información asociada a los cambios en la red y sus servicios de red, en cumplimiento con el Sistema de Gestión de Seguridad de la información.

4. GENERALIDADES

Con la finalidad de llevar una adecuada gestión de la conectividad interna de la red y sus servicios de red, el Área de Tecnologías de la Información realizara las siguientes acciones:

4.1. Para la seguridad de las conexiones y servicios de red, se mantiene implementado un firewall y antivirus

4.2. Todos los usuarios de PROINVERSION sin excepción deben acceder a la red, utilizando las credenciales asignadas

4.3. No se permite el acceso a la red interna de PROINVERSION y a sus servicios mediante el uso de redes inalámbricas

4.4. Se permite la conexión a redes mediante cableado a todo el personal que, por sus funciones, deba tener acceso

4.5. La red de conexiones VPN se utilizará para el cumplimiento del trabajo remoto y el acceso deberá realizarse mediante las credenciales asignadas

4.6. El tráfico hacia internet se encuentra controlado mediante firewall, el cual no permite protocolos utilizados para descargas P2P, ni el acceso a sitios no autorizados.

4.7. Se permite conexiones a la red inalámbrica de PROINVERSION para uso de terceros siempre y cuando el acceso se encuentre autorizado por el OSCD y no sea a la red interna

4.8. La red inalámbrica utilizada por terceros no debe permitir conectarse a la red interna de PROINVERSION, ni aplicaciones o desarrollos internos.

4.9. Los puntos de red que no estén siendo utilizados estarán deshabilitados.

4.10. Se debe garantizar la seguridad de la red mediante la separación de ambientes de procesamiento de información: ambiente de desarrollo, pruebas y producción.

4.11. Los usuarios son responsables del ingreso, actualización, calidad de datos y uso de credenciales de acceso a las diferentes aplicaciones y a la red.

4.12. Los usuarios son responsables de utilizar adecuadamente la red, con la finalidad de evitar congestión o degradación de los servicios asociados o que dependen de la infraestructura de red de PROINVERSION.

4.13. Se prioriza el uso de la infraestructura de red para el intercambio de información que sea de índole laboral

4.14. Los relojes de todos los sistemas de información deben estar sincronizados a una fuente oficial de tiempo, lo que permitirá manejar registro de logs exactos en fechas y horas

5. SECUENCIA DE ACTIVIDADES

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Evaluar seguridad de red y servicios de red			
1	Listar componentes de red y servicios de red - Revisar la configuración de red, valores y atributos establecidos de la red para mantener identificadas y especificadas las características de componentes y recursos que la conforman	Área de TI.	Especialista de Tecnologías de Información y Redes
2	Evaluar arquitectura de red - Revisar la distribución de la red y que su diagrama de red se encuentre actualizado	Área de TI.	Especialista de Tecnologías de Información y Redes
3	Evaluar servicios de red	Área de TI.	Especialista de Tecnologías de Información y Redes
4	Elaborar informe de evaluación de red	Área de TI.	Especialista de Tecnologías de Información y Redes
Formular propuesta de mejora de red y servicios de red			
5	Analizar informe de evaluación de red y servicios de red ¿Requiere implementación de mejoras? Si: Ir a tarea 6 No: Terminar proceso	Área de TI.	OSCD
6	Elaborar propuesta de implementación de mejoras en la red y sus servicios de red	Área de TI.	OSCD
Revisar propuesta de mejoras de red y servicios de red			
7	Revisar resultados de informe y propuesta de implementación de mejoras ¿Se tiene observaciones? Si: Ir a tarea 5 No: Ir a tarea 8	Área de TI.	Jefe de TI
8	Aprobar propuesta de mejora en la red y servicio de red	Área de TI.	Jefe de TI
Ejecutar mejoras a la red propuesta			
9	Planificar atención a la implementación de controles en la red ¿Es mejora en el servicio? Si: Ir a tarea 11 No: Ir a tarea 10	Área de TI.	Especialista de Tecnologías de Información y Redes
10	Implementar controles en la red	Área de TI.	Especialista de Tecnologías de Información y Redes
11	Coordinar mejoras en el servicio de red con los proveedores	Área de TI.	Especialista de Tecnologías de Información y Redes

12	Elaborar reporte de atención a la implementación de mejoras en la red y servicios de red	Área de TI.	Especialista de Tecnologías de Información y Redes
Certificar mejoras realizadas a la seguridad de red			
13	Revisar y dar conformidad a las actividades de implementación de controles en la red y sus servicios de red	Área de TI.	OSCD
14	Documentar los registros de atención a la solicitud de revisión y mejoras en red y sus servicios de red	Área de TI.	OSCD
Fin			

6. ANEXOS

6.1. Anexo 1 : Flujograma de procedimiento de seguridad de conectividad de la red interna y servicios de red

Anexo 1 : Flujograma de procedimiento de seguridad de conectividad de la red interna y servicios de red