PROCEDIMIENTO	Código: **S03.04.09.03**
	Versión: 01
	Vigencia: 24/09/2025
Dueño del proceso: Oficina de Administración	

GESTIÓN DE CODIGO MALICIOSO Y ANTIVIRUS

	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 14:54:22
	Víctor Chávez Gómez	Jefe de Tecnologías de la Información	Firmado digitalmente por: CHAVEZ GOMEZ Victor Hugo FAU 20380799643 soft Fecha: 23/09/2025 18:32:06
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 16:36:42
Aprobado por:	Alberto Blas Ortiz	Jefe de la Oficina de Administración	

Versión	Descripción de Cambios (indicar sección de corresponder)	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. **Antivirus:** Programa de software diseñado para proteger computadoras y otros dispositivos electrónicos contra software malicioso

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. **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”.

2.1.7. **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.

2.1.8. **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.

2.1.9. **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.

2.1.10. **Integridad:** Propiedad de exactitud y lo completo.

2.1.11. **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.

2.1.12. **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.

2.2. 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. Jefe de TI

3.1.1. Aprobar mejoras detectadas requeridas pos-remediación

3.2. Del Especialista de tecnologías de información y redes

3.2.1. Resolver incidencias asociados a identificación de virus informáticos y antimalware
3.2.2. Monitorear constantemente las consolas o herramientas antivirus
3.2.3. Atender oportunamente las detecciones de potenciales virus
3.2.4. Informar al OSCD periódicamente sobre la identificación de potenciales amenazas detectadas por las herramientas antivirus y antimalware

4. GENERALIDADES

4.1. Establecer medidas técnicas y organizativas para prevenir, detectar y responder a amenazas de malware, protegiendo la información y los sistemas de la organización.

4.2. La gestión de código malicioso y antivirus aplica a todos los sistemas, dispositivos (incluyendo equipos de usuarios), redes y software gestionados por PROINVERSION o accesibles desde su entorno

4.3. El software y las instalaciones de procesamiento de información son vulnerables a la introducción de software malicioso como, por ejemplo, virus informático, gusanos de red, troyanos y bombas lógicas. Se debe concientizar a los usuarios acerca de los peligros del software no autorizado o malicioso, y los administradores deben, cuando corresponda, introducir controles especiales para detectar o prevenir la introducción de estos

4.4. En la institución, el software instalado debe tener licencia, y se prohíbe el uso de software no autorizado.

4.5. La necesidad de uso de nuevo software “no licenciado” por parte de los usuarios debe ser informada al responsable de área o jefe de área correspondiente y aprobada por el OSCD, y en caso de ser necesario, por la jefatura de tecnología de información.

4.6. Se realizará revisiones periódicas del contenido de software y datos de los sistemas que sustentan procesos críticos de la institución. La presencia de archivos no aprobados o modificaciones no autorizadas será investigada formalmente.

4.7. Los planes de continuidad de los negocios contemplarán la recuperación respecto de ataques de virus, incluyendo todos los datos necesarios, el resguardo del software y las disposiciones para la recuperación.

4.8. Se debe configurar los equipos de cómputo con software base a nivel de seguridad de la información

4.9. Se prohíbe la obtención de software desde o a través de redes externas, hacia la red; salvo con autorización expresa del OSCD, quien señalará en dicho caso qué medidas de protección deberían tomarse.

4.10. El OSCD se apoyará en el área de TI para la evaluación del software obtenido desde o a través de redes externas, así como de nuevo software que requiera ser instalado desde un medio magnético

4.11. El personal no debe abrir archivos adjuntos en correos de remitentes desconocidos.

4.12. Se controlará la entrada de virus en la institución a través de los puntos de acceso con el exterior, tanto en los puntos compartidos (correo, web, transferencia de archivos, entre otros) como en los puntos locales (CDROM, discos externos, memorias flash, entre otros)

4.13. La red Interna y los sistemas de tratamiento de información disponen de software de detección y reparación antivirus, que se actualiza periódicamente, para examinar computadoras y medios informáticos, ya sea como medida de precaución o rutinaria.

4.14. Se revisará el cumplimiento de que esté configurada la actualización automática de la firma de antivirus en la última versión publicada por el fabricante.

4.15. El software antivirus estará configurado y actualizado teniendo en cuenta los siguientes puntos:

Configuración:

- Se analizará cualquier archivo existente en cualquier dispositivo de almacenamiento externo que se conecte al sistema (discos duros externos, memorias flash, CD's DVD's, entre otros)
- Se analizará cualquier archivo descargado a través del navegador desde Internet o cualquier red, como son páginas web, ejecutables, entre otros.
- Se analizará cualquier archivo adjunto a los correos electrónicos.

Actualización:

- La actualización de firmas y versiones será de manera automática y centralizada.
- El periodo de actualización de las firmas en los servidores y PC's o portátiles en caso existan se realizará automáticamente por lo menos una vez al día. En el caso de ordenadores portátiles no conectados permanentemente a la red de la institución, la actualización de las firmas se realizará por lo menos una vez al día en la fecha que se conecte.

4.16. Acción ante la detección de código malicioso:

- En el caso se detecte código malicioso que no ha sido eliminado o código malicioso que tiene una probabilidad significativa de comprometer las operaciones de la institución y de amenazar la seguridad de información, el supervisor de TI debe notificar de este evento de acuerdo con lineamientos establecidos de atención de Incidentes de Seguridad de Información. Asimismo, debe comunicar de este evento a los responsables de las plataformas para su acción inmediata.
- Los reportes generados por la herramienta Antivirus se depositarán en SharePoint destinado para estos casos para que puedan ser analizados por las áreas responsables con el objetivo de disminuir los eventos que atenten contra la disponibilidad, confidencialidad e integridad de los activos de información de la institución.

5. SECUENCIA DE ACTIVIDADES

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Revisar potenciales virus informático detectado			
1	Recopilar información del virus detectado • Mediante herramienta antivirus • Mediante detección manual (E. correo electrónico con archivo adjunto de fuente desconocida por los usuarios)	Área de TI	Especialista de Tecnología de Información y Redes
2	Evaluar fuentes de detección de virus informático o malware	Área de TI	Especialista de Tecnología de Información y Redes
3	Aislar equipo de red para evitar propagación y colocar en cuarentena archivos infectados en un entorno seguro	Área de TI	Especialista de Tecnología de Información y Redes
4	Identificar tipo de virus o malware	Área de TI	Especialista de Tecnología de Información y Redes
Ejecutar remediación de virus informático			
5	Erradicar amenaza detectada	Área de TI	Especialista de Tecnología de Información y Redes
6	Evaluar si los sistemas han sido comprometidos Si: Ir a la tarea 7 No: Ir a la tarea 8	Área de TI	Especialista de tecnología de información y redes
7	Restaurar sistema (reinstalando el Sistema Operativo)	Área de TI	Especialista de tecnología de información y redes
8	Restaurar servicio de TI	Área de TI	Especialista de tecnología de información y redes
9	Elaborar plan de mejora para reforzar la seguridad por remediación de virus informático o ransonware detectado	Área de TI	Especialista de tecnología de información y redes
Aprobar mejoras detectadas pos-remediación			
10	Evaluar plan de mejora propuesto ¿Se requiere aprobación? Si: Ir a tarea 11 No: Ir a tarea 9	Área de TI	Jefe de TI
11	Aprobar plan de mejora	Área de TI	Jefe de TI
Registrar mejoras aprobadas por remediación			
12	Registrar mejoras aprobadas para aplicar	Área de TI	Especialista de tecnología de información y redes
Fin			

6. ANEXOS

6.1. Procedimiento “Gestión de código malicioso y antivirus”

Anexo N° 2 : Procedimiento de Gestión de código malicioso y antivirus