San Isidro, 14 de Junio del 2024

RESOLUCIÓN DE GERENCIA GENERAL N° 000010-2024-SINEACE/CS-P-GG

VISTO:

El Informe N° 000007-2024-SINEACE/COSUSINEACE-P-GG-OTIC remitido por la Oficina de Tecnologías de la Información y Comunicaciones, el Informe N° 000042-2024-SINEACE/COSUSINEACE-P-GG-OPP remitido por la Oficina de Planificación y Presupuesto; y el Informe Legal N° 000048-2024-SINEACE/COSUSINEACE-P-GG-OAJ remitido por la Oficina de Asesoría Jurídica.

CONSIDERANDO:

Que, la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano;

Que, mediante la Resolución Directoral N° 022-2022-INACAL/DN del 29 de diciembre de 2022, se aprobó, entre otros, la Norma Técnica Peruana "NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información;

Que, por Resolución de Presidencia N° 000035-2023-SINEACE/P del 28 de febrero de 2023, se aprobó la "Directiva N° 000001-2023-SINEACE-P, Directiva que regula la elaboración, aprobación y actualización de documentos de gestión interna y orientadores en el Sineace";

Que, según el numeral 7.2.1 de la referida Directiva, corresponde a la Oficina de Planificación y Presupuesto, revisar las propuestas de directivas enviadas por las dependencias del Sineace y emitir un informe de opinión técnica;

Que, mediante Resolución de Presidencia N° 000003-2024-SINEACE/COSUSINEACE-P, publicada en el diario oficial "El Peruano", el 28 de febrero de 2024, se aprobó la Norma que define la estructura funcional no orgánica transitoria del Sineace, en su calidad de entidad en restitución, rectificada con Resolución de Presidencia N° 000016-2024-SINEACE/COSUSINEACE-P, cuyo literal e) del artículo 12 señala que forma parte de las funciones de la Gerencia General, aprobar las directivas u otros documentos de gestión interna;

Que, el literal d) del artículo 32 de la referida norma señala que forma parte de las funciones de la Oficina de Tecnologías de la Información y Comunicaciones, la elaboración y actualización de las normas institucionales para la gestión de recursos y seguridad informáticos;

Que, por Memorándum Múltiple N° 000009-2024-SINEACE/COSUSINEACE-P-GG del 24 de abril de 2024 se aprobó el "Lineamiento de Acceso al Servicio de VPN", documento que proporciona detalle sobre las disposiciones generales, actividades y productos de la asignación del servicio de VPN;

Que, mediante Informe N° 000007-2024-SINEACE/COSUSINEACE-P-OTIC del 15 de mayo de 2024, la Oficina de Tecnologías de la Información y Comunicaciones remitió a la Oficina de Planificación y Presupuesto la propuesta de la "Directiva que controla la Asignación del Servicio de VPN", a fin de continuar con el trámite correspondiente;

Que, mediante Informe N° 000042-2024-SINEACE/COSUSINEACE-P-GG-OPP del 24 de mayo de 2024, la Oficina de Planificación y Presupuesto brindó opinión favorable a la propuesta de "Directiva que controla la Asignación del Servicio de VPN". Asimismo, manifestó que dicha propuesta reemplazaría al "Lineamiento de Acceso al Servicio de VPN" aprobado con Memorándum Múltiple N° 000009-2024-SINEACE/COSUSINEACE-P-GG del 24 de abril de 2024; derivando el expediente a la Oficina de Asesoría Jurídica para la emisión del informe legal correspondiente;

Que, mediante Informe Legal N° 000048-2024-SINEACE/COSUSINEACE-P-GG-OAJ, del 30 de mayo de 2024, la Oficina de Asesoría Jurídica emitió opinión legal favorable a la propuesta de la Oficina de Tecnologías de la Información y Comunicaciones para la aprobación de la "Directiva que controla la Asignación del Servicio de VPN";

Con el visto bueno de la Oficina de Planificación y Presupuesto; de la Oficina de Asesoría Jurídica y de la Oficina de Tecnologías de la Información y Comunicaciones;

De conformidad con la Segunda Disposición Complementaria Final de la Ley N° 31520, Ley que Restablece la Autonomía y la Institucionalidad de las Universidades Peruanas; la Resolución de Presidencia N° 00003-2024-COSUSINEACE-P, que aprobó la Norma que define la estructura funcional no orgánica transitoria del Sineace, en su calidad de entidad en restitución, rectificada con Resolución de Presidencia N° 000016-2024-SINEACE/COSUSINEACE-P; y la Directiva N° 000001-2023-SINEACE-P, Directiva que regula la elaboración, aprobación y actualización de documentos de gestión interna y orientadores en el Sineace;

SE RESUELVE:

Artículo 1.- Aprobar la Directiva N° 000001-2024-SINEACE/CS-P-GG "Directiva que regula la red privada virtual o VPN", el mismo que forma parte integrante de la presente Resolución.

Artículo 2.- Dejar sin efecto el Memorándum Múltiple N° 000009-2024-SINEACE/COSUSINEACE-P-GG del 24 de abril de 2024 que aprobó el Lineamiento de Acceso al Servicio de VPN.

Artículo 3.- Disponer la publicación de la presente Resolución en la Plataforma Digital Única del Estado Peruano (www.gob.pe).

Regístrese, comuníquese y publíquese

Documento firmado digitalmente
NANCY JESUS TACILLA RAMIREZ
GERENTE GENERAL
Sineace

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"

San Isidro, 13 de Junio del 2024

DIRECTIVA N° 000001-2024-SINEACE/CS-P-GG

DIRECTIVA QUE REGULA LA RED PRIVADA VIRTUAL O VPN

1 OBJETIVO

Establecer las disposiciones para la asignación, atención y control del servicio de VPN (Red Privada Virtual) en el Sineace, siguiendo los lineamientos de seguridad de la información.

2 ALCANCE

Aplica a todos los servidores de la Oficina de Tecnologías de la Información y Comunicaciones (OTIC) y a todos los usuarios que tengan conexión remota segura a la red interna de la entidad mediante el uso de una red privada virtual (VPN).

3 BASE NORMATIVA

- Resolución de Presidencia N° 000003-2024-SINEACE/COSUSINEACE-P, que aprueba la "Norma que define la estructura funcional no orgánica transitoria del Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa – Sineace en su calidad de entidad en restitución".
- Resolución de Presidencia N° 035-2023-SINEACE/P, que aprueba la Directiva N° 000001-2023-SINEACE/P "Directiva para la formulación, aprobación y actualización de los documentos de gestión interna y orientadores del Sineace".
- Norma Técnica Peruana "NTP ISO/IEC 27001:2022 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información".
- Resolución Directoral N° 022-2022-INACAL/DN, que aprueba la NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.

4 DEFINICIONES

4.1. **Agente VPN:** Software de acceso remoto seguro (SSLVPN) que permite que los usuarios remotos puedan acceder de forma segura a los recursos de la red de la entidad a través de Internet.

4.2. **Ciberseguridad:** También conocida como seguridad informática, es la capacidad técnica para mantener y preservar el adecuado funcionamiento de las redes, activos y sistemas informáticos y protegerlos ante amenazas y vulnerabilidades en el entorno digital.

4.3. **Equipo de cómputo:** Tiene la capacidad de procesar datos, por ejemplo: computadora de escritorio, computadora portátil, tableta, entre otros.

4.4. **Información:** Activo esencial para el negocio de una organización y, por consiguiente, necesita ser debidamente protegido.

4.5. **Parches de seguridad:** Actualizaciones que se aplican para corregir errores de seguridad en programas o sistemas operativos. Son desarrolladas por el fabricante de software tras la detección de una vulnerabilidad y pueden instalarse de forma automática o manual.

4.6. **Seguridad de la información:** Cualquier activo que traslade, contenga o transfiera información (servidores virtuales, bases de datos, archivos, carpetas, aplicativos, repositorios electrónicos, configuraciones, entre otros) los cuales tienen como finalidad apoyar los procesos necesarios para el buen funcionamiento y la optimización del trabajo al interior de la Entidad.

4.7. **Usuario/a:** Personal que hace uso de los recursos informáticos de la entidad para llevar a cabo tareas específicas.

4.8. **VPN:** “Virtual Private Network” o Red Privada Virtual. Es una tecnología de red que permite crear una conexión segura y privada sobre Internet, encriptando los datos trasmitidos y protegiendo la información confidencial de posibles intercepciones o de monitoreo no autorizado.

5 RESPONSABILIDADES

5.1. La OTIC es responsable de:

a) Administrar y controlar los recursos y servicios informáticos, la asignación de VPN.
b) Proveer el soporte técnico necesario a fin de garantizar la disponibilidad de dichos recursos y servicios.
c) Cumplir y hacer cumplir la presente directiva.

5.2. Los/as usuarios/as de la VPN son responsables de:

a) Informar, mediante correo electrónico dirigido al servicio de Mesa de Ayuda, itservices@sineace.gob.pe, en el caso de suscitarse modificaciones de hardware, software, alertas de virus en el equipo de cómputo asociado al servicio de VPN que alteren las características que constituyen los requisitos técnicos mínimos, y que fueron objeto de verificación previo a la configuración de acceso a dicho servicio.

b) Realizar el cierre de sesión del servicio de VPN cada vez que culmine su trabajo en el equipo de cómputo.
c) Participar en charlas de concientización, brindadas por la OTIC, relacionadas a buenas prácticas en seguridad de la información, a fin de asegurar el buen uso de los equipos de cómputo durante el teletrabajo.

6 DISPOSICIONES GENERALES

6.1. Los equipos de cómputo para realizar teletrabajo pueden ser personales o asignados por la entidad, y deben contar con los mecanismos de seguridad necesarios, establecidos en la presente directiva.

6.2. A través del servicio de VPN se obtiene acceso remoto a las aplicaciones de la entidad, a los que el/la servidor/a tenga acceso autorizado y previamente configurado en su equipo.

7 DISPOSICIONES ESPECÍFICAS

7.1. Del acceso a la VPN

7.1.1. De la solicitud de acceso a la VPN

Si el equipo de cómputo es de uso personal:

a) El/la usuario/a debe solicitar mediante correo electrónico con copia a su Jefe/a inmediato/a superior, la revisión de los requisitos mínimos de seguridad, dirigido a itservices@sineace.gob.pe.

Si el equipo cómputo es asignado por la Entidad:

a) El/la usuario/a debe solicitar acceso a la VPN mediante correo electrónico adjuntando el registro **"Solicitud de Acceso al Servicio VPN" (F-OTI-12)**, dirigido a itservices@sineace.gob.pe.

b) El/la Analista en Servicios de TI debe revisar que el formato esté completo y firmado, el cual debe contar con la firma de el/la Jefe/a inmediato/a superior. Además, dicha solicitud debe contar con el número de contacto del/de la usuario/a.

7.1.2. De la revisión de los requerimientos de seguridad

Si el equipo de cómputo es de uso personal:

a) El/la Analista en Servicios de TI debe asignar personal de soporte técnico para la revisión del equipo de cómputo.

b) Soporte técnico debe revisar que el equipo de cómputo cuente con los siguientes requerimientos mínimos de seguridad:

- Sistema Operativo (SO) 10 en adelante, con licencia original y activada.
- SO con Parches de Seguridad actualizados.
- Software Antivirus con licencia original, actualizado y ejecutándose.
- Navegador web recomendable como Google Chrome, Mozilla Firefox o Microsoft Edge.

c) Soporte técnico debe informar mediante correo electrónico al/a la usuario/a solicitante, con copia al/a la Especialista en Infraestructura Tecnológica, al/a la Jefe/a de OTIC y al/a la Oficial de Seguridad y Confianza Digital, sobre la revisión del equipo. De encontrarse observaciones, éstas deben ser subsanadas por el/la usuario/a y solicitar una nueva revisión del equipo.

d) De ser conforme la revisión, el/la usuario/a debe solicitar acceso a la VPN mediante correo electrónico, adjuntando el registro **"Solicitud de Acceso al Servicio VPN" (F-OTI-12)**, dirigido a itservices@sineace.gob.pe.

e) El/la Analista en Servicios de TI debe revisar que el formato esté completo y firmado, el cual debe contar con la firma del/de la Jefe/a inmediato/a superior. Además, dicha solicitud debe contar con el número de contacto del/de la usuario/a.

Si el equipo de cómputo es asignado por la entidad:

a) El/la Analista en Servicios de TI debe asignar personal de soporte técnico para la revisión del equipo de cómputo.

b) Soporte técnico debe revisar que el equipo de cómputo cuente con los requerimientos mínimos de seguridad:

- SO con parches de seguridad actualizados.
- Software Antivirus actualizado y ejecutándose.

c) Soporte técnico debe informar mediante correo electrónico al/a la Especialista en Infraestructura Tecnológica, con copia al/a la Oficial de Seguridad y Confianza Digital y al/a la Jefe/a de la OTIC, sobre la revisión del equipo de cómputo.

7.1.3. De la configuración del acceso a la VPN y de la actualización del registro

El/la Especialista en Infraestructura Tecnológica debe realizar la configuración del acceso a la VPN y actualizar el registro "Inventario de Accesos a la VPN".

Si el equipo de cómputo es de uso personal:

a) Soporte técnico debe dar aviso al/ a la usuario/a solicitante mediante correo electrónico sobre la fecha de instalación y configuración del agente VPN.

7.1.4. De la instalación del agente VPN

a) Soporte técnico debe instalar y configurar el agente VPN en el equipo de cómputo de el/la usuaria/a.
b) Soporte técnico debe dar aviso del trabajo finalizado al/a la usuario/a mediante correo electrónico.

7.2. Del uso de la VPN

7.2.1. La OTIC cancelará la VPN a los/las usuarios/as que no registren actividad durante un periodo igual o mayor a los sesenta (60) días calendario.

7.2.2. El acceso a las carpetas compartidas en red solo está disponible para el/la usuario/a que utilice el equipo asignado por la entidad; siempre y cuando tenga acceso autorizado. Sin embargo, el/la usuario/a podrá hacer uso de las herramientas de colaboración en la nube asignadas por la entidad (OneDrive) para el acceso, tratamiento o almacenamiento de la información institucional bajo sus competencias.

7.3 **De las prohibiciones y recomendaciones sobre el uso de la VPN**

7.3.1 Son prohibiciones:

a) Facilitar u ofrecer la cuenta de usuario a terceras personas.
b) Utilizar la VPN para propósitos ajenos a las labores o actividades desarrolladas en el Sineace.
c) Divulgar la información recibida sobre el acceso y uso de la VPN del Sineace.
d) Navegar en sitios o páginas web que pongan en riesgo la información de la entidad a la que accede el/la usuario/a, como sitios de descargas de video, películas, software y música gratuita, entre otros.
e) Prestar el equipo de cómputo asignado por la entidad a personas distintas al/al usuario/a.

7.3.2 Son recomendaciones:

a) Bloquear su equipo (Windows + L) cada vez que se retire momentáneamente de su estación de trabajo, a fin de evitar que otras personas accedan al mismo y usen indebidamente la VPN.

b) Conectar su equipo por cable de red para mantener la estabilidad de la VPN.
c) El/la usuario/a que utilice equipo de cómputo de uso personal, debe evitar instalar y hacer uso de software no licenciado.

8. DISPOSICIONES COMPLEMENTARIAS

8.1 De requerirse soporte técnico posteriormente relacionado al acceso o el uso de la VPN, se debe comunicar mediante correo electrónico al servicio de Mesa de Ayuda: itservices@sineace.gob.pe.

8.2 La OTIC debe resolver las situaciones y aspectos no previstos en la presente Directiva.

9. FORMATOS

Formato: F-OTI-12 Solicitud de Acceso al Servicio VPN.

Sineace	FORMATO	F-OTI-012
	SOLICITUD DE ACCESO AL SERVICIO VPN	Versión: 02
		Página 1 de 1

USUARIO RESPONSABLE QUE RECEPCIONA	
APELLIDOS Y NOMBRES	
TELÉFONO DE CONTACTO	
SEDE	
DEPENDENCIA	
SUSTENTO	
MODALIDAD	

EQUIPO DE CÓMPUTO

ASIGNADO POR LA ENTIDAD ☐ DE USO PERSONAL ☐

VIGENCIA DE ACCESO

1 MES ☐ 2 MESES ☐

HORARIOS DE ACCESO

(8x5) 8:15AM - 5:15PM ☐ (18x7) 6:00AM - 23:59PM ☐ 24x7x365 ☐

ACCESOS

☐ ACCESOS DE ESCRITORIO REMOTO DESDE REDES EXTERNAS

CLÁUSULAS DE ACCESO A VPN

1. Sólo los usuarios previamente autorizados podrán utilizar los beneficios del Sistema VPN, y serán responsables del uso correcto del servicio de acceso remoto, accesos compartidos, entre otros.
2. Es responsabilidad del usuario con privilegios VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo de quien ha sido asignado con dichos privilegios.
3. Los accesos se habilitan según la vigencia y horarios establecidos en lo solicitado.
4. El aplicativo de VPN será configurado y administrado por el área de OTIC.
5. Las cuentas de usuario serán auditadas en el caso ocurriera algún evento de pérdida de información o alguna violación en la seguridad informática.
6. Los usuarios son responsables de cumplir con lo establecido en la Directiva que regula el servicio de VPN de Sineace.

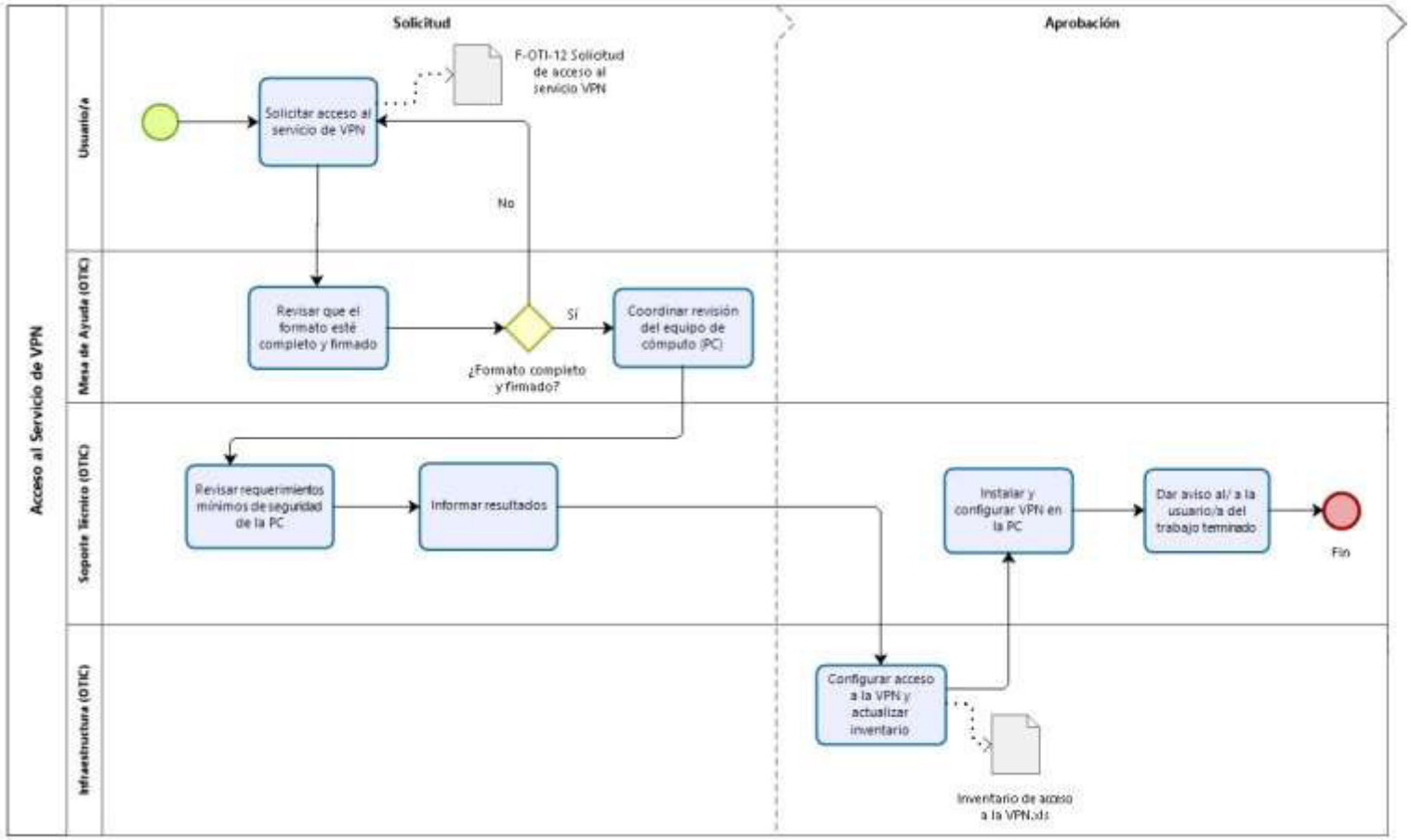
ACEPTO	NO ACEPTO
☐	☐

FIRMA DE EL/LA JEFE/A INMEDIATO/A

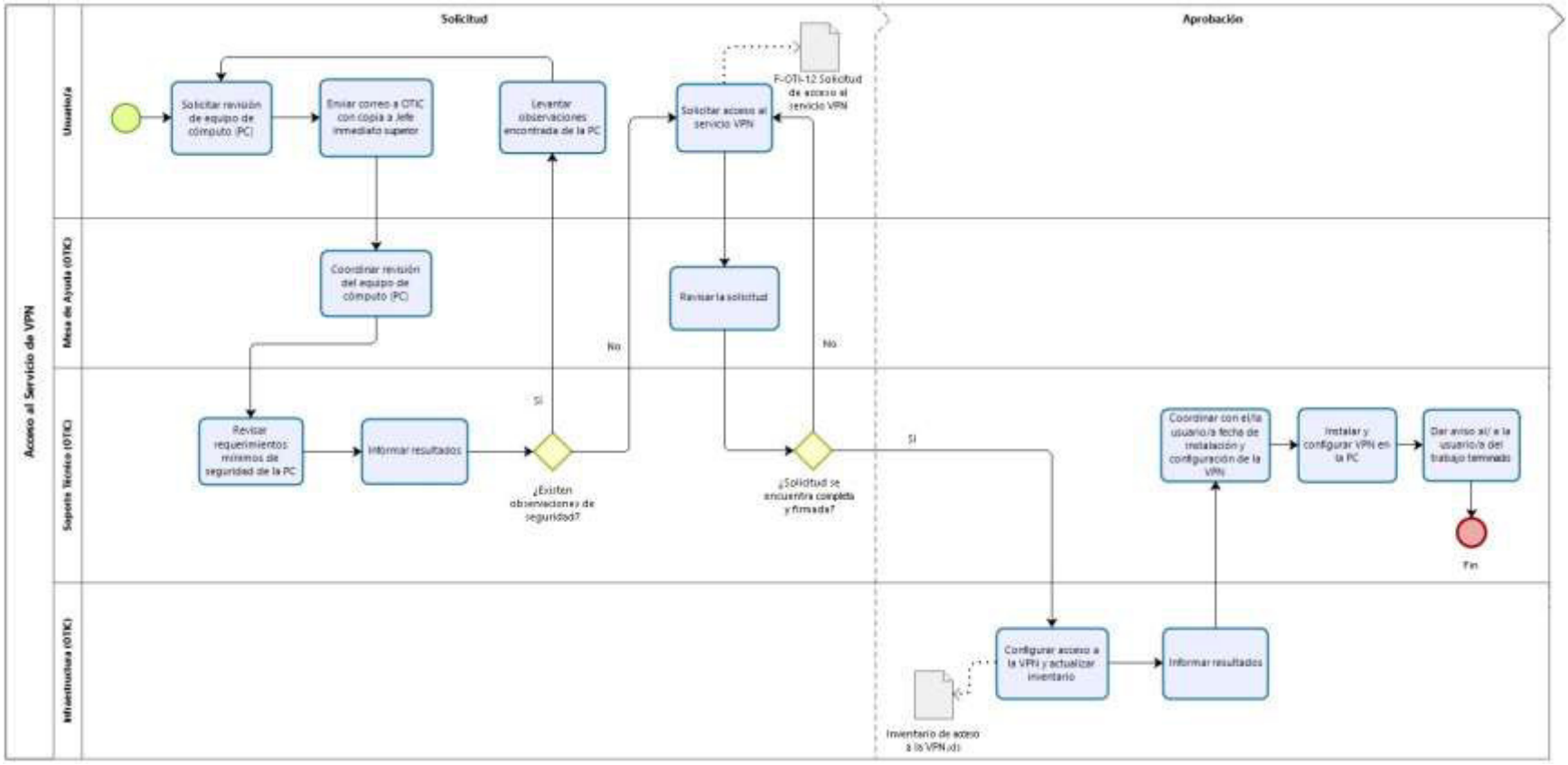
FIRMA DE EL/LA USUARIO/A

10. DIAGRAMA DE PROCESO

a) Equipo asignado por la Entidad



b) Equipo Personal



11. HOJA DE CONTROL DE CAMBIOS

N°	Versión	Descripción del cambio	Numeral(es) modificado(s)
		Versión inicial del documento	