Resolución Directoral

N° 07-2023-VIVIENDA/OGEI

Lima, 08 de noviembre del 2023

VISTO:

El informe Nº 62-2023-VIVIENDA/OGEI-GFN del Oficial de Seguridad de la Información;

CONSIDERANDO:

Que, mediante Decreto Supremo N° 004-2013-PCM, se aprueba la Política Nacional de Modernización de la Gestión Pública, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principales y lineamientos para una actuación coherente y eficaz del sector público, al servicio de los ciudadanos y el desarrollo del país; agregando en el numeral 3.2 los ejes transversales de la Política de Modernización en el Gobierno Electrónico;

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 Resolución Ministerial N° 004-2016-PCM, modificada por Resolución Ministerial N° 166-2017-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición" en todas las entidades integrantes del Sistema Nacional de Informática, en concordancia con la recomendación efectuada, a través del Memorando N° 152-2015-PCM/ONGEI, por la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros;

Que, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, establece el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, el artículo N° 105 del Reglamento del Decreto Legislativo N° 1412, aprobado por Decreto Supremo N° 029-2021-PCM, establece como parte de las obligaciones de las entidades públicas en seguridad digital, que implementen y mantengan un sistema de Gestión de Seguridad de la Información. Asimismo, el artículo N° 109 del mismo cuerpo normativo dispone, entre otros, que el diseño, implementación, operación y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) atiende a las necesidades de todas las partes interesadas de la entidad y responde a los objetivos estratégicos, estructura, tamaño, procesos y servicios de la entidad;

Que, el artículo 55 del Reglamento de Organización y Funciones - ROF del Ministerio de Vivienda, Construcción y Saneamiento MVCS, establece que la Oficina General de Estadística e Informática - OGEI, es el órgano encargado responsable de la gestión de la infraestructura de tecnologías de la información y comunicaciones, así como planificar, desarrollar, implementar y

gestionar proyectos de desarrollo de soluciones basadas en tecnologías de la información y comunicación para la administración y gestión de la informática estadística sectorial;

Que, con Resolución Ministerial Nº 356-2018-VIVIENDA, del 23 de octubre de 2018 se constituyó el Comité de Gobierno Digital en el marco de la Resolución Ministerial N° 119-2018-PCM, entre cuyas funciones destaca la de liderar y dirigir el proceso de transformación digital en la entidad;

Que, el artículo 1 de la Resolución Directoral N° 022-2022-INACAL/DN, del 29 de diciembre de 2022, se aprueba la norma técnica peruana NTP-ISO/IEC 27002:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2a Edición Reemplaza a la NTP-ISO/IEC 27002:217;

Que, estando a lo expuesto y conforme a la propuesta remitida por el Oficial de Seguridad de la Información, contando con la opinión favorable de la Oficina de Tecnologías de la Información, corresponde expedir la presente Resolución, según lo expresado en el documento de visto;

De conformidad con lo dispuesto en la Ley N°29518, Ley Orgánica del Poder Ejecutivo, Ley N° 30156, Ley de Organización y Funciones del Ministerio de Vivienda, Construcción y Saneamiento; y su Reglamento de Organización y Funciones, aprobado por Decreto Supremo N° 010-2014-VIVIENDA, modificado por Decreto Supremo N° 006-2016-VIVIENDA, la Resolución Ministerial N° 004-2016-PCM que aprueba la Norma Técnica Peruana “NTP ISO/IEC 27001:2014;

SE RESUELVE:

Artículo 1.- Aprobar los siguientes Documentos de Gestión de Seguridad de la Información, el mismo que forma parte integrante de la presente Resolución.

N°	Documento	Código	Versión
1	Procedimiento de Control de Atención de PC's con problemas de antivirus	DGSI-08	1.0
2	Procedimiento de Atención de VPN	DGSI-09	1.0

Artículo 2.- Disponer la publicación de la presente Resolución en el Portal Institucional del Ministerio de Vivienda, Construcción y Saneamiento.

Regístrese y comuníquese

FIRMA DIGITAL
VIVIENDA
Firmado digitalmente por: SUCA ANCACHI Helmer Efrain FAU 20504743307 hard
Motivo: Soy el autor del documento
Fecha: 2023/11/08 14:26:19-0500

Ing. HELMER EFRAIN SUCA ANCACHI
Director General
Oficina General de Estadística e Informática

PROCEDIMIENTO DE CONTROL DE ATENCIÓN DE PC'S CON PROBLEMAS DE ANTIVIRUS

Nombre	Cargo	Visto
Elaborado por: Guillermo Pedro Fernández Namuche	Especialista en Seguridad de la Información	FIRMA DIGITAL Firmado digitalmente por:FERNÁNDEZ NAMUCHE Guillermo Pedro FAU 20504743307 soft Motivo: En señal de conformidad Fecha: 2023/11/07 09:18:52-0500
Revisado por: Maria Isabel Vasquez Aldave	Directora de la OTI	FIRMA DIGITAL Firmado digitalmente por:VASQUEZ ALDAVE Maria Isabel FAU 20504743307 soft Motivo: Soy el autor del documento Fecha: 2023/11/07 16:53:33-0500
Kenny Mirko Rodriguez Cáceres	Coordinador de Infraestructura	FIRMA DIGITAL Firmado digitalmente por:RODRIGUEZ CACERES Kenny Mirko FAU 20504743307 soft Motivo: En señal de conformidad Fecha: 2023/11/07 11:26:27-0500
José Uilises Jordan Liza	Soporte técnico	FIRMA DIGITAL Firmado digitalmente por:JORDAN LIZA Jose Ulises FAU 20504743307 soft Motivo: Soy el autor del documento Fecha: 2023/11/07 11:04:24-0500
Aprobado por: Helmer Efrain Suca Ancachi	Director General de la OGEI	FIRMA DIGITAL Firmado digitalmente por:SUCA ANCACHI Helmer Efrain FAU 20504743307 hard Motivo: En señal de conformidad Fecha: 2023/11/08 10:29:35-0500

FICHA DE INDICADOR DE DESEMPEÑO

Código del proceso	PR-OTI.007
Nombre del proceso	Elaboración de normativas y procedimientos de tecnologías de información y comunicaciones
Objetivo del proceso	Mejorar de la capacidad de gestión y control de atención de PC's con problemas de antivirus
Nombre del proceso relacionado	Documento de control

I. INDICADOR

Nombre del Indicador	Cantidad de normas de seguridad aprobadas
Objetivo del Indicador	Medir la cantidad de normas de seguridad elaboradas por la Oficina de Tecnología de la información
Fórmula	Sumatoria de la cantidad de normas de seguridad propuesta que han sido aprobadas
Unidad de Medida	Normas de seguridad aprobadas
Frecuencia	Anual
Línea Base	Corresponde a la cantidad de normas de seguridad elaboradas por la Oficina de Tecnología de la Información
Meta	N.D.
Fuente de datos	Oficina de Tecnología de la Información
Responsabilidad	Oficina de Tecnología de la Información / Oficina General de Estadística e Informática

II. OBJETIVO DEL PROCEDIMIENTO

Establecer las disposiciones para el control de atención de PC's con problemas de antivirus en el Ministerio de Vivienda, Construcción y Saneamiento, reduciendo los riesgos en la seguridad de la información.

III. ALCANCE DEL PROCEDIMIENTO

Las disposiciones contenidas en este procedimiento son de aplicación y obligatorio cumplimiento para la Oficina General de Estadística e Informática, y todo usuario que

tengan acceso a los servicios materia del presente procedimiento, para el desarrollo de sus funciones.

IV. BASE NORMATIVA

- Mediante Decreto Supremo N° 004-2013-PCM, se aprueba la Política Nacional de Modernización de la Gestión Pública, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principales y lineamientos para una actuación coherente y eficaz del sector público, al servicio de los ciudadanos y el desarrollo del país; agregando en el numeral 3.2 los ejes transversales de la Política de Modernización en el Gobierno Electrónico;

- Que, mediante Resolución Ministerial N° 004-2016-PCM, modificada por Resolución Ministerial N° 166-2017-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición" en todas las entidades integrantes del Sistema Nacional de Informática, en concordancia con la recomendación efectuada, a través del Memorando N° 152-2015-PCM/ONGEI, por la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros;

- 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. Requisitos. 3ª Edición Reemplaza a la NTP-ISO/IEC 27001:2014; y deja sin efecto la NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2ª Edición.

V. SIGLAS Y DEFINICIONES

- **Activos de información:** Conocimiento o datos que tienen valor para el individuo u organización[1].
- **Aplicativo:** Programa informático que facilita las tareas de procesamiento, consulta, modificación, eliminación o reportes sobre las bases de datos de información del MVCS y que es manejado por usuarios específicos.
- **GLPI:** Solución libre de gestión de servicios de tecnología de la información, un sistema de seguimiento de incidencias y de solución service desk.
- **MVCS:** Ministerio de Vivienda, Construcción y Saneamiento.
- **NTP-ISO/IEC 27001:2022**: Es una norma técnica peruana que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización.

[1] Tomado de la Norma ISO/IEC 27032:2012 (definición 4.6, traducida al español), disponible en Internet en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.

- **Información:** Es un activo que, como otros activos importantes del negocio, es esencial para el negocio de una organización y, por consiguiente, necesita ser debidamente protegida.
- **OTI:** Oficina de Tecnología de la Información.
- **OGEI:** Oficina General de Estadística e Informática.
- **Proveedor de servicios de aplicaciones:** Operador que proporciona una solución alojada que proporciona servicios de aplicaciones que incluyen modelos de entrega basados en web o cliente-Servidor.
- **Seguridad de la información:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (servidores virtuales, bases de datos, archivos, carpetas, aplicativos, repositorios electrónicos, configuraciones, entre otros), los cuales tienen como finalidad apoyar las tareas misionales y administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Entidad[2].

VI. CONSIDERACIONES PREVIAS

- Infraestructura deberá enviar el reporte de estado de los equipos con problemas de antivirus indicando.

VII. ROLES Y RESPONSABILIDADES

- **Infraestructura:** es el responsable de la administración de la consola del antivirus en el MVCS. Identifica y reporta los equipos con problema de antivirus.

- **Mesa de Servicio:** es el responsable de asignar el requerimiento de revisión de los equipos con problemas de antivirus. Verifica y asigna requerimiento.

- **Soporte:** Revisa, atiende y comunica resultados.

- **Oficial de Seguridad de la Información:** es el encargado de la supervisión del cumplimiento del presente procedimiento.

VIII. MATRIZ RACI

Cuadro N° 01 - Matriz RACI

Roles / Actividades	Infraestructura	Mesa de Servicio	Soporte
Identificar los equipos con problemas de antivirus y actualización	R		

[2] Tomado del Portal de ISO 27001 en español, Gestión de Seguridad de la Información. En http://www.iso27000.es/glosario.html#section10a

Envíar reporte mediante correo del estado de las PC´s con problemas de antivirus y/o actualizaciones	R	I	
Asignar requerimiento y verificar las PC´s indicadas en el reporte de estado		R	I
Revisar PC´s y atender requerimiento		I	R
Comunicar la culminación del requerimiento asignado	I	I	R
Escalar a proveedor	R	I	

Leyenda:
R = Responsabilidad | A = Autoriza | I = Informado | C = Consultado

IX. PROCEDIMIENTO

N°	Actividad	Entrada	Salida	Herramienta	Responsable
1	**INICIO** **IDENTIFICA LOS EQUIPOS CON PROBLEMAS DE ANTIVIRUS Y ACTUALIZACIÓN** Mediante la administración de la consola del antivirus, se identifican las PC's con problemas de antivirus y/o actualización.	Identificación de PC's con problemas	Reporte	Consola del antivirus	Infraestructura (Responsable de la administración de la consola antivirus)
2	**ENVÍA REPORTE MEDIANTE CORREO DEL ESTADO DE LAS PC´S CON PROBLEMAS DE ANTIVIRUS Y/O ACTUALIZACIONES** Se realiza un reporte de las PC´s con problemas de antivirus y/o actualización, indicando el nombre del usuario, nombre del equipo, área y la descripción del estado.	Reporte con las descripción de los estados	Reporte	Correo	Infraestructura (Responsable de la administración de la consola antivirus)
3	**ASIGNA REQUERIMIENTO Y VERIFICA LAS PC'S INDICADAS EN EL REPORTE DE ESTADO** Mesa de Servicio con el reporte de las PC´s con problemas de antivirus, asigna a técnico para la verificación correspondiente.	Asignación de técnico	Ticket de atención por GLPI	GLPI	Mesa de Servicio
4	**REVISA PC´S Y ATIENDE REQUERIMIENTO** El técnico de soporte técnico, revisa la PC y atiende la solicitud de acuerdo al requerimiento.	Revisa PC	Atiende solicitud	Instalador y agente de antivirus	Soporte (Técnico de soporte asignado)

5	**COMUNICA LA CULMINACIÓN DEL REQUERIMIENTO ASIGNADO** ¿Persisten la PC con problemas de antivirus? **No**, comunica mediante correo electrónico la culminación del requerimiento asignado. **Si**, se realiza el escalamiento del requerimiento al proveedor. Regresar al paso 1 **FIN**	Culminación de trabajo realizado	Respuesta	Correo	Soporte
6	**ESCALAMIENTO A PROVEEDOR** Si la PC después de ser revisada por el técnico de soporte, persiste con el problema de antivirus; se realiza el escalamiento al proveedor del antivirus. Después de haber obtenido la solución, se regresa al paso 3.	Culminación de trabajo realizado	Correo	Correo	Infraestructura (Responsable de la administración de la consola antivirus)

X. JUSTIFICACIÓN

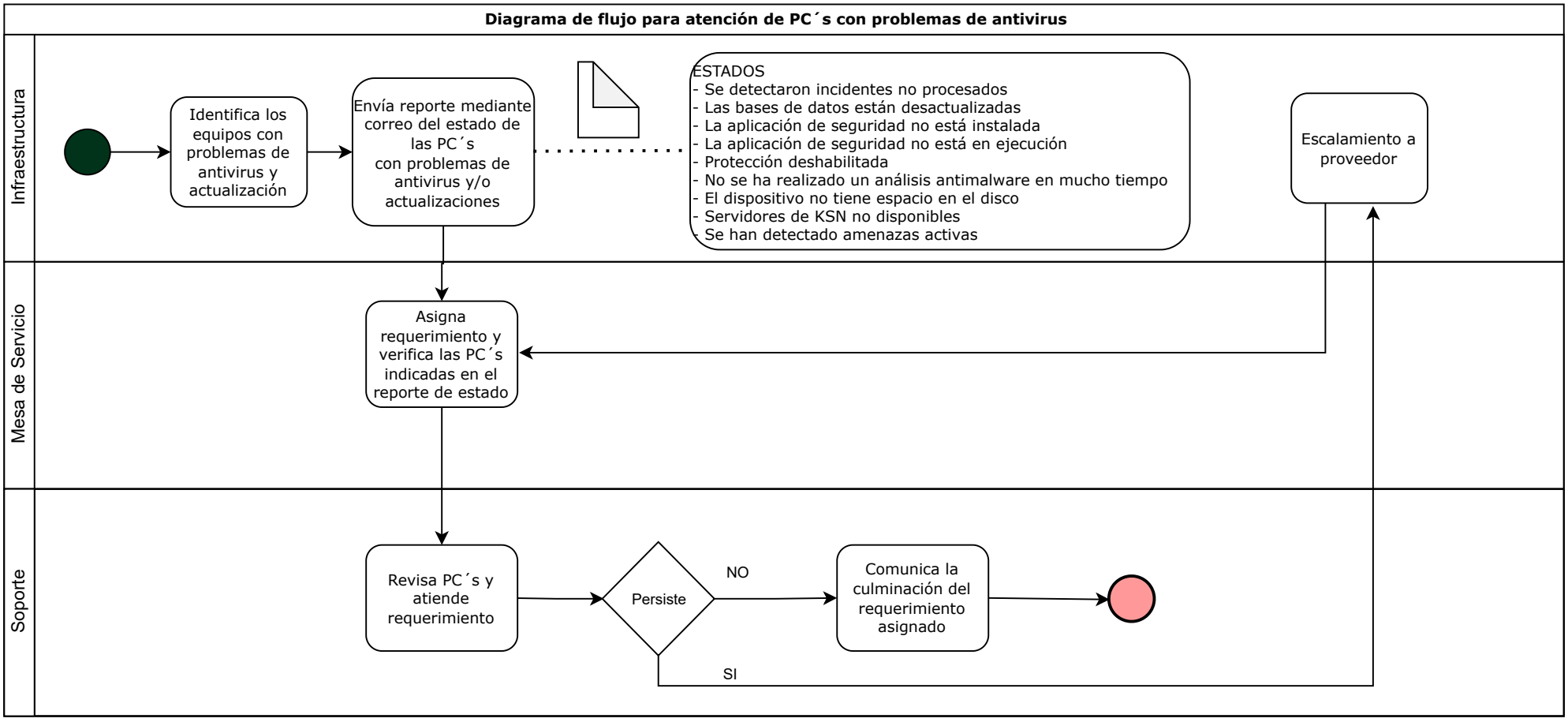
En la ISO 27001:2022 **"Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información"**, cuyo principal objetivo es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

El propósito de dicho control es garantizar que la información y otros activos de información asociados están protegidos contra malware.
En su guía indica que la protección contra el malware debe basarse en software de detección y reparación del malware, conciencia de seguridad de la información, acceso al sistema adecuado y controles de gestión de cambios. El uso de software de detección y reparación de malware por sí solo, no suele ser adecuado.

XI. SUPERVISIÓN

La supervisión del cumplimiento del presente procedimiento estará a cargo del Oficial de Seguridad de la Información del MVCS. Es su responsabilidad solicitar cada meses un informe a la OTI de las acciones realizadas y presentar a la OGEI un informe de cumplimiento.

XII. ANEXO (Diagrama de flujo)



NOTA: El área de Infraestructura es el responsable de la administración de la consola del antivirus en el MVCS

FIRMA DIGITAL
Firmado digitalmente por:FERNÁNDEZ NAMUCHE Guillermo Pedro FAU 20504743307 soft
Motivo: En señal de conformidad
Fecha: 2023/10/11 15:03:03-0500

FIRMA DIGITAL
Firmado digitalmente por:RODRIGUEZ CACERES Kenny Mirko FAU 20504743307 soft
Motivo: Soy el autor del documento
Fecha: 2023/10/11 15:15:39-0500

FIRMA DIGITAL
Firmado digitalmente por:JORDAN LIZA Jose Ulises FAU 20504743307 soft
Motivo: En señal de conformidad
Fecha: 2023/10/11 15:27:43-0500

MVCS
Por: VASQUEZ ALDAVE Maria Isabel FAU 20504743307 soft
Motivo: Doy V° B°
Fecha: 2023/10/17 17:19:06-0500

PROCEDIMIENTO DE ATENCIÓN DE VPN

Nombre	Cargo	Visto
Elaborado por: Guillermo Pedro Fernández Namuche	Especialista en Seguridad de la Información	FIRMA DIGITAL Firmado digitalmente por:FERNÁNDEZ NAMUCHE Guillermo Pedro FAU 20504743307 soft Motivo: En señal de conformidad Fecha: 2023/11/07 09:19:47-0500
Revisado por: Maria Isabel Vasquez Aldave	Directora de la OTI	FIRMA DIGITAL Firmado digitalmente por:VASQUEZ ALDAVE Maria Isabel FAU 20504743307 soft Motivo: Soy el autor del documento Fecha: 2023/11/07 16:46:05-0500
Kenny Mirko Rodriguez Cáceres	Coordinador de Infraestructura	FIRMA DIGITAL Firmado digitalmente por:RODRIGUEZ CACERES K Mirko FAU 20504743307 soft Motivo: En señal de conformidad Fecha: 2023/11/07 11:25:19-0500
José Uilises Jordan Liza	Soporte técnico	FIRMA DIGITAL Firmado digitalmente por:JORDAN LIZA Jose Ulises FAU 20504743307 soft Motivo: Soy el autor del documento Fecha: 2023/11/07 11:03:25-0500
Aprobado por: Helmer Efrain Suca Ancachi	Director General de la OGEI	FIRMA DIGITAL Firmado digitalmente por:SUCA ANCACHI Helmer Efrain FAU 20504743307 hard Motivo: En señal de conformidad Fecha: 2023/11/08 10:30:43-0500

FICHA DE INDICADOR DE DESEMPEÑO

Código del proceso	PR-OTI.007
Nombre del proceso	Elaboración de normativas y procedimientos de tecnologías de información y comunicaciones
Objetivo del proceso	Mejorar de la capacidad de gestión y control de atención de VPN
Nombre del proceso relacionado	Documento de control

I. INDICADOR

Nombre del Indicador	Cantidad de normas de seguridad aprobadas
Objetivo del Indicador	Medir la cantidad de normas de seguridad elaboradas por la Oficina de Tecnología de la información
Fórmula	Sumatoria de la cantidad de normas de seguridad propuesta que han sido aprobadas
Unidad de Medida	Normas de seguridad aprobadas
Frecuencia	Anual
Línea Base	Corresponde a la cantidad de normas de seguridad elaboradas por la Oficina de Tecnología de la Información
Meta	N.D.
Fuente de datos	Oficina de Tecnología de la Información
Responsabilidad	Oficina de Tecnología de la Información / Oficina General de Estadística e Informática

II. OBJETIVO DEL PROCEDIMIENTO

Establecer las disposiciones para el control y atención de VPN en el Ministerio de Vivienda, Construcción y Saneamiento, reduciendo los riesgos en la seguridad de la información.

III. ALCANCE DEL PROCEDIMIENTO

Las disposiciones contenidas en este procedimiento son de aplicación y obligatorio cumplimiento para la Oficina General de Estadística e Informática, y todo usuario que

tengan acceso a los servicios materia del presente procedimiento, para el desarrollo de sus funciones.

IV. BASE NORMATIVA

- Mediante Decreto Supremo N° 004-2013-PCM, se aprueba la Política Nacional de Modernización de la Gestión Pública, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principales y lineamientos para una actuación coherente y eficaz del sector público, al servicio de los ciudadanos y el desarrollo del país; agregando en el numeral 3.2 los ejes transversales de la Política de Modernización en el Gobierno Electrónico;

- Que, mediante Resolución Ministerial N° 004-2016-PCM, modificada por Resolución Ministerial N° 166-2017-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición" en todas las entidades integrantes del Sistema Nacional de Informática, en concordancia con la recomendación efectuada, a través del Memorando N° 152-2015-PCM/ONGEI, por la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros;

- 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. Requisitos. 3ª Edición Reemplaza a la NTP-ISO/IEC 27001:2014; y deja sin efecto la NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2ª Edición.

V. SIGLAS Y DEFINICIONES

- **Activos de información:** Conocimiento o datos que tienen valor para el individuo u organización[1].
- **Checklist:** Un checklist o lista de comprobación es una herramienta escrita que se utiliza para esquematizar la información concerniente a una tarea, un proceso o cualquier conjunto de elementos pendientes, de manera tal de poder controlar sencilla y rápidamente su ejecución.
- **GlobalProtect:** Permite crear políticas precisas para restringir o autorizar el acceso según la necesidad empresarial, independientemente de que los usuarios se conecten desde dentro o fuera de la organización.
- **MVCS:** Ministerio de Vivienda, Construcción y Saneamiento.

[1] Tomado de la Norma ISO/IEC 27032:2012 (definición 4.6, traducida al español), disponible en Internet en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.

- **Información:** Es un activo que, como otros activos importantes del negocio, es esencial para el negocio de una organización y, por consiguiente, necesita ser debidamente protegida.
- **NTP-ISO/IEC 27001:2022**: Es una norma técnica peruana que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización.
- **OTI:** Oficina de Tecnología de la Información.
- **OGEI:** Oficina General de Estadística e Informática.
- **Parches de seguridad:** Los parches de seguridad son actualizaciones que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Estas actualizaciones son desarrolladas por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden instalarse de forma automática o manual.
- **Proveedor de servicios de aplicaciones:** Operador que proporciona una solución alojada que proporciona servicios de aplicaciones que incluyen modelos de entrega basados en web o cliente-Servidor.
- **Seguridad de la información:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (servidores virtuales, bases de datos, archivos, carpetas, aplicativos, repositorios electrónicos, configuraciones, entre otros), los cuales tienen como finalidad apoyar las tareas misionales y administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Entidad[2].
- **VPN:** Redes privadas virtuales son una herramienta importante para proteger su privacidad y seguridad en línea.

VI. CONSIDERACIONES PREVIAS

- La Mesa de Servicio debe verificar los formatos enviados por los colaboradores CAS/FAG/Practicante, el cual debe incluir el VB del/a Director/a, debe estar marcado la casilla de VPN y debe estar marcado y llenado la casilla de condición laboral.
- La Mesa de Servicio debe verificar los formatos enviados por las Órdenes de Servicios, el cual debe incluir el VB de/a Director/a, debe estar marcado la casilla de VPN, debe estar marcado y llenado la casilla de condición laboral, así como sustentar el requerimiento.

VII. ROLES Y RESPONSABILIDADES

- **Mesa de Servicio:** es el responsable de asignar el requerimiento de revisión de los equipos con problemas de antivirus. Verifica y asigna requerimiento.

[2] Tomado del Portal de ISO 27001 en español, Gestión de Seguridad de la Información. En http://www.iso27000.es/glosario.html#section10a

- **Soporte:** Revisa los requerimientos mínimos de la PC, atiende y comunica resultados.
- **Infraestructura:** es el responsable de registrar y/o actualizar el "Inventario de acceso a la VPN".
- **Oficial de Seguridad de la Información:** es el encargado de la supervisión del cumplimiento del presente procedimiento.

VIII. MATRIZ RACI

Cuadro N° 01 - Matriz RACI

Roles / Actividades	Colaborador del MVCS	Mesa de Servicio	Soporte	Infraestructura
Envía formato de altas y bajas de cuentas de usuarios solicitando VPN vía correo electrónico	R	I		
Verifica formato. La solicitud debe contar con número de contacto del usuario		R		
Comunica al colaborador las observaciones a subsanar	I	R		
Asigna personal de soporte		R	I	
Verifica PC si cuenta con los requerimiento mínimos de seguridad			R	
Informa mediante correo electrónico el trabajo de la verificación realizado			R	I
Instala y configura el GlobalProtect en la PC del usuario y responde correo electrónico con el trabajo finalizado	I		R	I
Habilita acceso a la VPN y registra y/o actualiza el "Inventario de acceso a la VPN"			I	R
Responde correo electrónico con el trabajo realizado			I	R

Leyenda:
R = Responsabilidad | **I** = Informado | **H** = Habilita

IX. PROCEDIMIENTO

N°	Actividad	Entrada	Salida	Herramienta	Responsable
1	**INICIO** **ENVÍA FORMATO DE ALTAS Y BAJAS DE CUENTAS DE USUARIOS SOLICITANDO VPN VIA CORREO ELECTRONICO** El/a colaborador/a envía mediante correo electrónico el formato de altas y bajas, solicitando acceso a la VPN	Envío de formato	Formato	Correo	Colaborador del MVCS
2	**VERIFICA FORMATO. LA SOLICITUD DEBE CONTAR CON NUMERO DE CONTACTO DEL USUARIO** Mesa de servicio verifica el formato, el cual debe contar con el VB del Director/a, estar marcado la casilla de VPN, condición laboral y sustentar el requerimiento si es OS	Verificación de información de acuerdo al formato	Está conforme o no está conforme	Correo	Mesa de Servicio
3	**COMUNICA AL COLABORADOR LAS OBSERVACIONES A SUBSANAR** La Mesa de Servicio de acuerdo a la verificación del formato de altas y bajas, comunica al colaborador/a	De acuerdo a la verificación	Comunica al colaborador /a	Correo	Mesa de Servicio
4	**ASIGNA PERSONAL DE SOPORTE** La Mesa de Servicio asigna personal de soporte para la verificación del equipo	Asignación de técnico	Ticket de atención por GLPI	Correo	Mesa de Servicio
5	**VERIFICA PC SI CUENTA CON LOS REQUERIMIENTOS MÍNIMOS DE SEGURIDAD** El técnico de soporte revisa la PC para verificar si cuenta con los requerimientos mínimos de seguridad: - Sistema Operativo (SO) 10 para adelante - Parches de seguridad del SO actualizado - Antivirus actualizado y ejecutándose	Revisa PC	Atiende solicitud	Revisión Visual	Soporte
6	**INFORMA MEDIANTE CORREO ELECTRÓNICO EL TRABAJO DE LA VERIFICACIÓN REALIZADO** Soporte informa mediante correo electrónico, el trabajo realizado y si está conforme o no	Culminación de trabajo realizado	Respuesta	Correo	Soporte

7	**CONFIGURACIÓN ACCESO A LA VPN Y REGISTRA Y/O ACTUALIZA EL "INVENTARIO DE ACCESOS A LA VPN** Infraestructura realiza la configuración del acceso de la VPN, asimismo actualiza el inventario de acceso en la Hoja de Cálculo	Configuración de Acceso	Registro	Hoja de Cálculo	Infraestructura
8	**RESPONDE CORREO ELECTRÓNICO CON EL TRABAJO REALIZADO** Infraestructura responde mediante correo electrónico la finalización del trabajo realizado	Culminación de trabajo realizado	Respuesta	Correo	Infraestructura
9	**INSTALA Y CONFIGURA EL GLOBALPROTECT EN LA PC DEL USUARIO Y RESPONDE CORREO ELECTRÓNICO CON EL TRABAJO REALIZADO** Soporte instala y configura el Globalprotect en la PC del colaborador	Configuración de la VPN	Respuesta	Globalprotect y correo	Soporte

X. JUSTIFICACIÓN

En la ISO 27001:2022 **"Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información"**, cuyo principal objetivo es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

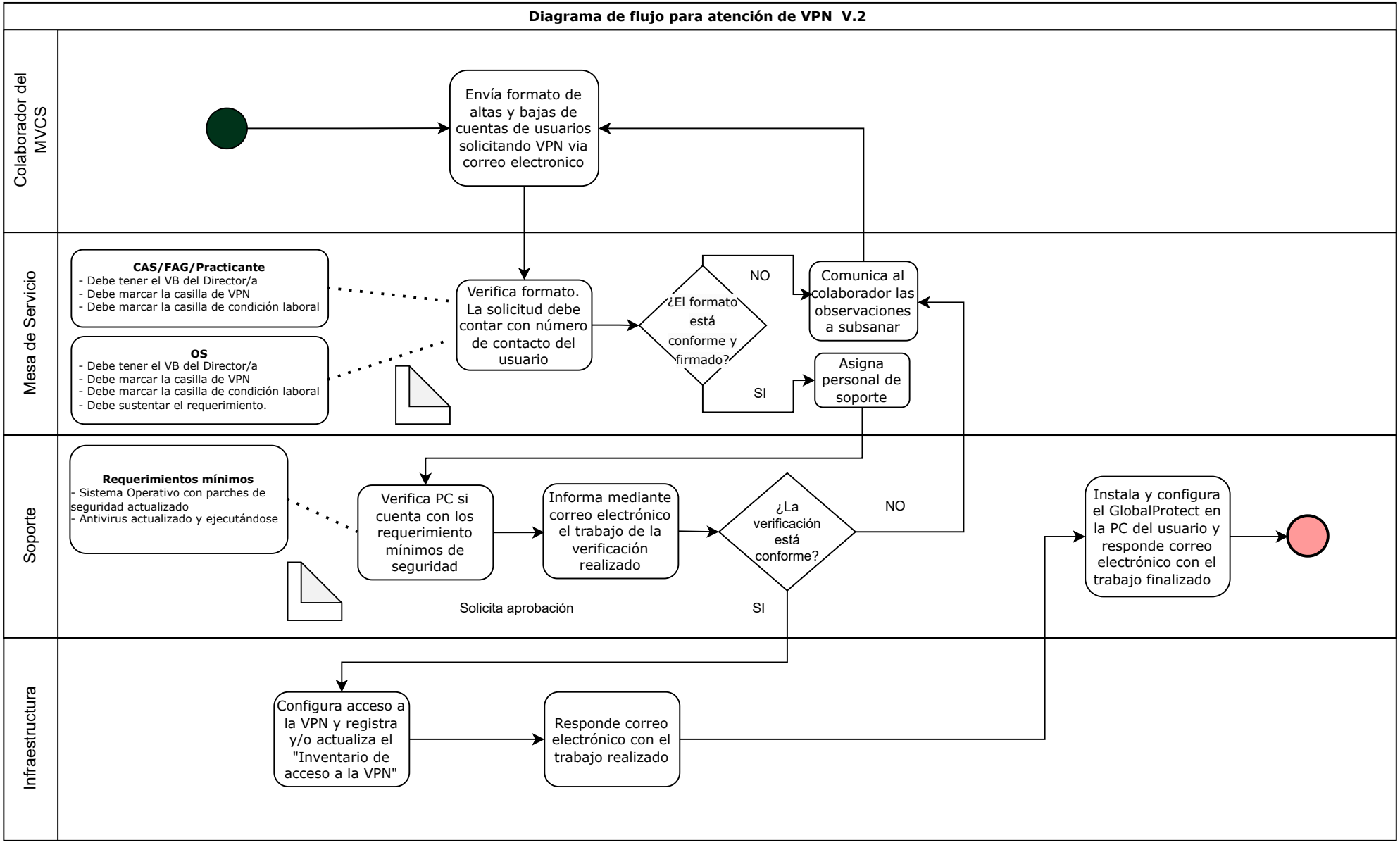
El propósito de dicho control es garantizar que los datos se transmitan de forma segura y que solo las personas autorizadas tengan acceso a ellos, realizando controles necesarios para mitigar los riesgos y amenazas.

XI. SUPERVISIÓN

La supervisión del cumplimiento del presente procedimiento estará a cargo del Oficial de Seguridad de la Información del MVCS. Es su responsabilidad solicitar cada meses un informe a la OTI de las acciones realizadas y presentar a la OGEI un informe de cumplimiento.

XII. ANEXO (Diagrama de flujo)

Diagrama de flujo para atención de VPN V.2



NOTA: El área de Infraestructura es el responsable de registrar y/o actualizar el "Inventario de acceso a la VPN"