Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0303 Versión: ***04*** Fecha: 24/07/2023

NOMBRE DEL PROCEDIMIENTO	Atención de solicitud de servicio de tecnologías de la información

APROBACIÓN		
Nombre y cargo	**Órgano o Unidad Orgánica**	**Firma y sello**
Elaborado por: César Gamarra Malca Jefe de la Oficina de Tecnologías de la Información	Oficina de Tecnologías de la Información	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: GAMARRA MALCA Cesar Guillermo FAU 20521286769 soft Cargo: Jefe de la Oficina de Tecnologías de la Información Lugar: Sede Central - Jesus Maria - Lima - Lima Motivo: Soy el autor del documento Fecha/Hora: 24/07/2023 16:28:27
Revisado por: Pamela Roxana Meza Pinto Jefa de la Oficina de Planeamiento y Presupuesto	Oficina de Planeamiento y Presupuesto	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: MEZA PINTO Pamela Roxana FAU 20521286769 soft Cargo: Jefa de la Oficina de Planeamiento y Presupuesto Lugar: Sede Central - Jesus Maria - Lima - Lima Motivo: Soy el autor del documento Fecha/Hora: 24/07/2023 15:58:09
Revisado por: Manuel Roberto De la Flor Matos Jefe (e) de la Oficina de Asesoría Jurídica	Oficina de Asesoría Jurídica	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: DE LA FLOR MATOS Manuel Roberto FAU 20521286769 soft Cargo: Jefe de la Oficina de Asesoría Jurídica Lugar: Sede Central - Jesus Maria - Lima - Lima Motivo: En señal de conformidad Fecha/Hora: 24/07/2023 15:44:11
Aprobado por: José Manuel Zavala Muñoz Gerente General	Gerencia General	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: ZAVALA MUÑOZ Jose Manuel FAU 20521286769 soft Cargo: GERENTE GENERAL (SECRETARIA GENERAL) Lugar: Sede Central - Jesus Maria - Lima - Lima Motivo: En señal de conformidad Fecha/Hora: 25/07/2023 17:11:02

CONTROL DE CAMBIOS		
Versión	**Sección del Procedimiento**	**Descripción del cambio**
00	-	Versión inicial del procedimiento[1]

[1] Aprobado mediante Resolución de Gerencia General N° 075-2019-OEFA/GEG de fecha 31 de diciembre de 2019.

Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0303 Versión: ***04*** Fecha: 24/07/2023

CONTROL DE CAMBIOS		
Versión	**Sección del Procedimiento**	**Descripción del cambio**
01	Todas las secciones	- Se actualiza el objetivo, alcance. - Se incorporan normas a la base normativa. - Se modifican las consideraciones generales. - Se actualiza de actividades. - Se incorpora el Formato PA0303-F01 *"Seguimiento de Mejoras"*. - Se incorpora los instructivos Instructivo I-OTI-PA0303-1: *"Instructivo de atención de incidentes y problemas de TI"* e Instructivo I-OTI-PA0303-2: *"Instructivo de atención de solicitud de servicio de TI"*.[2]
02	Actualización a las actividades del procedimiento	- Se actualiza la base normativa, - Se realiza la precisión en la actividad números 1, 4, 5, 9, 11 y 13 del procedimiento. - Se realizó la actualización a los instructivos I-OTI-PA0303-1 Instructivo de atención de incidentes y problemas de TI y al I-OTI-PA0303-2 Instructivo de atención de solicitud de servicio de TI.[3]
03	Alcance, Definiciones, Consideraciones Generales, Anexos del procedimiento	- Se realizan precisiones en el alcance, la base normativa, consideraciones generales, definiciones y en la actividad N° 2. - Se realizó la actualización a los instructivos I-OTI-PA0303-1 Instructivo de atención de incidentes, problemas, eventos y debilidades; y, al I-OTI-PA0303-2 Instructivo de atención de solicitud de servicio de TI[4].
04	***Actividades*** ***Anexos del procedimiento***	- ***Se realiza una precisión a la Actividad N° 7*** - ***Se actualiza el Instructivo I-OTI-PA0303-2: "Instructivo de atención de solicitud de servicio de TI.*** - **Se incorpora el instructivo *I-OTI-PA0303-3 Instructivo de Gestión de Incidentes de Seguridad y Ciberseguridad.*** - ***Se adecua el versionamiento de los formatos y anexos a la versión del procedimiento[5].***

OBJETIVO	Establecer las actividades que permitan gestionar las solicitudes de servicio de tecnologías de la información y asegurar su atención dentro de los plazos establecidos.
ALCANCE	El presente procedimiento es de aplicación obligatoria para la Oficina de Tecnologías de la Información y las áreas del OEFA. Comprende desde el ingreso de la solicitud hasta la evaluación del servicio.
RESPONSABLE DEL PROCEDIMIENTO	Jefe/a de la Oficina de Tecnologías de la Información
BASE NORMATIVA	- Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la administración pública. - Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital. - Decreto Supremo N° 024-2006-PCM, Decreto Supremo que aprueba el Reglamento de la Ley N° 28612, Ley que norma el uso, adquisición y adecuación del software en la administración pública.

[2] Modificado mediante la Resolución N° 051-2021-OEFA/GEG de fecha 09 de junio de 2021.

[3] Modificado mediante la Resolución N° 00063-2022-OEFA/GEG de fecha 26 de mayo de 2022.

[4] Modificado mediante la Resolución de Gerencia General N° 00114-2022-OEFA/GEG de fecha 22 de diciembre de 2022.

[5] ***Modificado mediante la Resolución de Gerencia General N° 00062-2023-OEFA/GEG de fecha 24 de julio de 2023.***

	- Decreto Supremo N° 103-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030. - Decreto Supremo N° 013-2017-MINAM, que aprueba el Reglamento de Organización y Funciones del Organismo de Evaluación y Fiscalización Ambiental - OEFA - Decreto Supremo N° 051-2018-PCM, Decreto Supremo que crea el Portal de software Público Peruano y establece disposiciones adicionales sobre el software Público Peruano. - Resolución Ministerial N° 073-2004-PCM, que aprueba la Guía para la Administración Eficiente del Software Legal en la Administración Pública. - Resolución Ministerial N° 004-2016-PCM, que 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. - Resolución Ministerial N° 041-2017-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana *"NTP ISO/IEC 12207:2016 - Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software. Tercera Edición"*, en todas las entidades integrantes del Sistema Nacional de Informática. - Resolución de Secretaría de Gobierno Digital N° 001-2019-PCM-SEGDI, que aprueba la Directiva N° 001-2019-PCM-SEGDI, *"Directiva para compartir y usar Software Público Peruano"*. - Resolución de Presidencia del Consejo Directivo N° 00020-2022-OEFA/PCD, que aprueba la designación y funciones del Oficial de Seguridad y Confianza Digital del OEFA. - Resolución de Gerencia General N° 00092-2022-OEFA/GEG, que conforma el Equipo de Respuesta ante incidentes de seguridad digital del OEFA. Las referidas normas incluyen sus modificatorias.
CONSIDERACIONES GENERALES	- La solicitud de servicio de tecnologías de información es canalizada a través del aplicativo de mesa de ayuda que permite visualizar la trazabilidad de todas las solicitudes. - Cuando las solicitudes de servicios tecnológicos se encuentren vinculadas al Banco de Datos Personales del OEFA, se debe considerar lo siguiente: • El/la Oficial de Seguridad y Confianza Digital notifica, mediante correo institucional, a el/la Oficial de Datos Personales, el estado de los incidentes. • El/La Oficial de Seguridad y Confianza Digital revisa con el/la Oficial de Datos Personales los aspectos legales que los incidentes puedan ocasionar al OEFA.
DEFINICIONES	- **Acuerdo de Nivel de Servicio:** Acuerdo escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. - **Aplicativo de mesa de ayuda:** Aplicativo informático que permite el registro y seguimiento de las solicitudes de servicios de tecnologías de la información. - **Catálogo de servicios de TI:** Base de datos o documento estructurado que contiene información sobre todos los servicios vigentes e incluye aquellos que se pueden implementar, forma parte del aplicativo de mesa de ayuda. - **Evento de seguridad de información:** Ocurrencia identificada de un sistema o servicio que determine una posible infracción de los compromisos de Seguridad de la Información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad de información. - **Debilidad:** Defecto o vulnerabilidad sobre un activo o un control de información que puede dejarlo expuesto ante una amenaza. - **Incidentes:** Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio. - **Problema:** Causa desconocida de uno o más incidentes, un incidente que no tiene su causa raíz identificada acaba transformándose ***en*** un problema. - **Modelo de atención:** Documento donde se encuentran las tareas a ejecutarse de acuerdo a una programación para cada solicitud de servicio. - **Solicitud de servicio:** Solicitud que hace un/a usuario/a reportando incidentes, requerimientos, cambios o peticiones. - **Usuario/a:** Servidor/a civil, contratista, tercero/a contratado/a, practicante preprofesional, practicante profesional y secigrista, que tenga vínculo laboral o contractual con la Entidad; o, se encuentre en alguna modalidad formativa, según corresponda; y, use habitualmente el hardware y software brindados por el OEFA.

Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0303 Versión: ***04*** Fecha: 24/07/2023

SIGLAS	- ANS: Acuerdo de Nivel de Servicio - OTI: Oficina de Tecnologías de la Información - TI: Tecnologías de la información

REQUISITOS PARA INICIAR EL PROCEDIMIENTO	
Descripción del requisito	**Fuente**
Solicitud de atención de servicios de TI	Áreas usuarias

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
1	Recibir y registrar la solicitud de servicio de TI	Recibe y registrar la solicitud de servicio de TI, según lo siguiente: Si la solicitud se realiza por correo institucional o llamada telefónica: la registra en el aplicativo de mesa de ayuda y va a la actividad N° 2. Si la solicitud se realiza por el aplicativo de mesa de ayuda: va a la actividad N° 3. **Plazo:** Un (1) día hábil, luego de recibida la solicitud.	Solicitud de atención	Operador/a de soporte	OTI
2	Identificar el tipo de la solicitud	Identifica el tipo de solicitud. - En caso se trate de una solicitud de servicios de TI, va la actividad N° 3. - En caso se trate de un Incidente, problema, evento y debilidad, procede de acuerdo con lo señalado en el I-OTI-PA0303-1 *"Instructivo de atención de incidentes, problemas, eventos y debilidades"* y va a la actividad N° 6.	Reporte del registro de la Solicitud	Operador/a de soporte	OTI
3	Clasificar la solicitud de servicio de TI y verificar si se requiere aprobación para su atención	Clasifica la solicitud de servicio de TI en base al catálogo de servicios de TI. Verifica si la solicitud de servicio de TI requiere aprobación para su atención. **¿Requiere aprobación?** **Sí:** Va a la actividad N° 4. **No:** Va a la actividad N° 6. Cambia el estado de la solicitud a *"en espera"*.	Catálogo de servicios de TI	Operador/a de soporte	OTI
4	Enviar la solicitud para su aprobación	Envía la solicitud, mediante correo institucional, para su aprobación conforme al catálogo de servicios de TI.	Correo institucional	Operador/a de soporte	OTI

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
		En caso que apruebe el/la Jefe/a de la OTI o el/la Jefe/a del Área usuaria va a la actividad N° 5. **Plazo:** Un (1) día hábil luego de la clasificación de la solicitud de servicio de TI.			
5	Evaluar y aprobar la solicitud	Evalúa y aprueba la solicitud mediante correo institucional. **¿La solicitud es conforme?** **Sí:** Va a la actividad N° 6. **No:** Va a la actividad N° 11.	-	Jefe/a	OTI
6	Asignar la solicitud para su atención	Asigna la solicitud a el/la Especialista de ***la*** OTI para su atención. **Plazo:** Un (1) día hábil desde su aprobación. Cambia el estado de la solicitud a *"asignado en curso"*.	Solicitud asignada en curso	Operador/a de soporte	OTI
7	Revisar y atender la solicitud asignada	Revisa la solicitud asignada y la atiende conforme a lo dispuesto en ***los*** Instructivos I-OTI-PA0303-2 *"Instructivo de atención de solicitud de servicio de TI"* y el ***I-OTI-PA0303-3 Instructivo de Gestión de Incidentes de Seguridad y Ciberseguridad"*** y a los plazos dispuestos del ANS que se encuentran en el Catálogo de Servicios. **¿La solicitud fue atendida?** **Sí:** Va a la actividad N° 8. **No:** Va a la actividad N° 6.	Catálogo de servicios de TI	Analista de OTI	OTI
8	Actualizar el estado de la solicitud	Actualiza el estado de la solicitud con el resultado de las acciones realizadas. Cambia el estado de la solicitud a *"Resuelto"*. *Nota:* *El aplicativo de mesa de ayuda envía automáticamente una encuesta al el/la usuario/a para que indique su nivel de satisfacción respecto a la calidad de servicio brindado.*	-	Analista de OTI	OTI
9	Cerrar el registro de la solicitud	El/La Analista de ***la*** OTI cierra el registro de la solicitud, el/la operador/a de soporte genera el reporte de gestión de solicitudes mediante el Aplicativo de Mesa de Ayuda.	Reporte de gestión de solicitudes del Aplicativo de mesa de ayuda	Analista de ***la*** OTI Operador/a de soporte	OTI

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
		El/La Operador/a de soporte realiza el seguimiento diario y mediante correo institucional comunica a los/as responsables (Analistas de ***la*** OTI) para el cierre de los tickets. **Plazo:** Un (1) hábil luego de atendida la solicitud. Cambia el estado de la solicitud a *"cerrado"*.			
10	Analizar los resultados de las encuestas	Analiza los resultados de las encuestas de atención de los requerimientos. Dicho análisis se realiza mensualmente.	Reporte de encuestas	Analista de procesos de TI	OTI
11	Identificar y coordinar acciones de mejora	Identifica y coordina, mediante correo institucional, con el/la Supervisor/a de soporte técnico las posibles soluciones de mejora a implementar.	Correo Institucional	Analista de procesos de TI	OTI
12	Evaluar y comunicar la viabilidad de las acciones de mejora	Evalúa y comunica a el/la Jefe/a de la OTI, mediante correo institucional, la viabilidad de las acciones de mejora propuestas. **¿Es viable?** **Sí:** Va a la actividad N° 13. **No:** Va a la actividad N° 11.	Correo Institucional	Supervisor/a de soporte técnico	OTI
13	Registrar e implementar las acciones de mejora y revisar resultados	Registra la mejor propuesta en el PA0303-F01: *"Seguimiento de Mejoras"* e implementa las acciones para la mejora del servicio y revisa los resultados.	PA0303-F01: *"Seguimiento de Mejoras"*	Analista de OTI	OTI
14	Verificar la efectividad de las mejoras del servicio	Verifica la efectividad de las mejoras implementadas, de acuerdo con el PA0303-F01 *"Seguimiento de Mejoras"*. **¿Es conforme?** **Sí:** Va a la actividad N° 15. **No:** Va a la actividad N° 13.	PA0303-F01: *"Seguimiento de Mejoras"*	Analista de procesos de TI	OTI
15	Comunicar y registrar la acción implementada de mejora	Comunica, mediante correo institucional, a el/la Jefe/a de la OTI la acción implementada de mejora y lo registra en el PA0303-F01 *"Seguimiento de Mejoras"*. Fin del procedimiento.	Correo institucional PA0303-F01: *"Seguimiento de Mejoras"*	Analista de procesos de TI	OTI

DOCUMENTOS QUE SE GENERAN:

Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0303
		Versión: ***04***
		Fecha: 24/07/2023

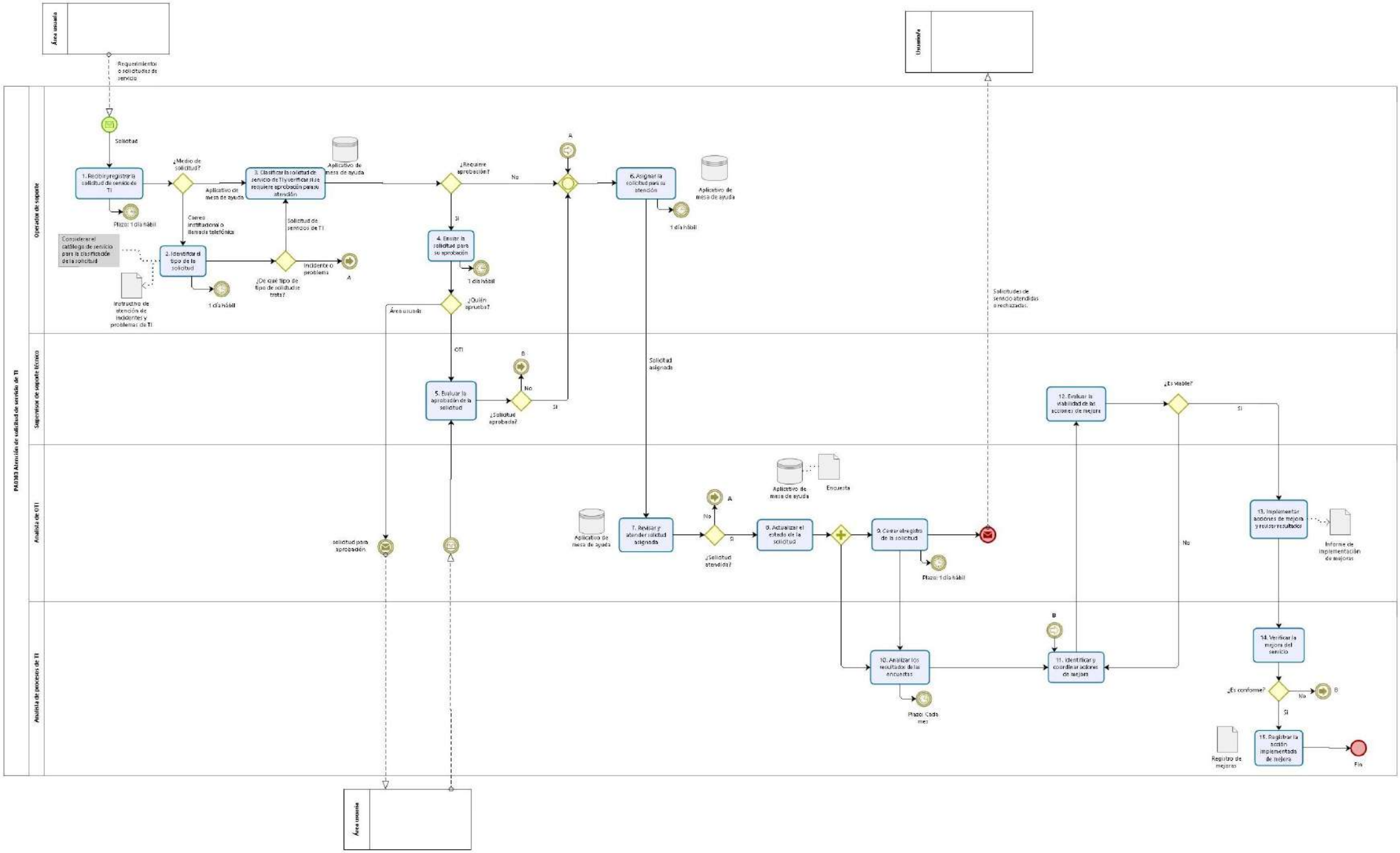
Seguimiento de Mejoras
Reporte de encuestas del aplicativo de mesa de ayuda
Reporte del registro de la solicitud
Reporte de gestión de solicitudes del aplicativo de mesa de ayuda

ANEXOS DEL PROCEDIMIENTO:

- Anexo N° 1: Diagrama del proceso
- Anexo N° 2: Formato PA0303-F01: *"Seguimiento de Mejoras"*
- Anexo N° 3: Instructivo I-OTI-PA0303-1: *"Instructivo de atención de incidentes, problemas, eventos y debilidades"*
- *Anexo N° 4:* Instructivo I-OTI-PA0303-2: *"Instructivo de atención de solicitud de servicio de TI"*
- *Anexo N° 5:* ***Instructivo I-OTI-PA0303-3: "Instructivo de incidentes de seguridad y ciberseguridad"***

PROCESO RELACIONADO

PA03 - Tecnologías de la información


PA0303 Atención de solicitud de servicio de TI
Área usuaria
Requerimientos o solicitudes de servicio
Usuario/a
Operador de soporte
Supervisor de soporte técnico
Analista de OTI
Analista de procesos de TI
Solicitud
1. Recibir y registrar la solicitud de servicio de TI
Plazo: 1 día hábil
¿Medio de solicitud?
Aplicativo de mesa de ayuda
Correo institucional o llamada telefónica
3. Clasificar la solicitud de servicio de TI y verificar si es requiere aprobación para su atención
Aplicativo de mesa de ayuda
Solicitud de servicios de TI
Considerar el catálogo de servicio para la clasificación de la solicitud
2. Identificar el tipo de la solicitud
1 día hábil
Instructivo de atención de incidentes y problemas de TI
¿De qué tipo de tipo de solicitud se trata?
Incidente o problema
A
¿Requiere aprobación?
No
Sí
4. Enviar la solicitud para su aprobación
1 día hábil
¿Quién aprueba?
Área usuaria
OTI
5. Evaluar la aprobación de la solicitud
¿Solicitud aprobada?
No
Sí
B
A
6. Asignar la solicitud para su atención
Aplicativo de mesa de ayuda
1 día hábil
Solicitud asignada
Solicitudes de servicio atendidas o rechazadas.
solicitud para aprobación
Aplicativo de mesa de ayuda
7. Revisar y atender solicitud asignada
¿Solicitud atendida?
No
Sí
A
Aplicativo de mesa de ayuda
Encuesta
8. Actualizar el estado de la solicitud
9. Cerrar registro de la solicitud
Plazo: 1 día hábil
10. Analizar los resultados de las encuestas
Plazo: Cada mes
B
11. Identificar y coordinar acciones de mejora
12. Evaluar la viabilidad de las acciones de mejora
¿Es viable?
Sí
No
13. Implementar acciones de mejora y revisar resultados
Informe de implementación de mejoras
14. Verificar la mejora del servicio
¿Es conforme?
No
B
Sí
15. Registrar la acción implementada de mejora
Registro de mejoras
Fin
Área usuaria

Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0303 Versión: ***04*** Fecha: 24/07/2023

Segumiento de mejoras								
N°	**Procedimiento**	**Descripción de la Mejora**	**Acción a implementar**	**Responsable de implementación**	**Fecha de identificación de mejoras**	**Fecha de cierre de mejora**	**Estado**	**Comentarios**

Instructivo de atención de incidentes, problemas, eventos y debilidades

I. OBJETIVO

Establecer las acciones para la ejecución de la atención y respuesta de incidentes, problemas, así como la comunicación sobre eventos y debilidades en el OEFA, asegurando que se mantienen los mejores niveles posibles de calidad y disponibilidad.

II. INSTRUCCIONES

2.1. Requerimientos, incidentes y problemas operativos

2.1.1. El/La usuario/a solicita la atención de requerimiento, incidente y problemas operativos a la mesa de ayuda, a través de los medios: soporte@oefa.gob.pe y números de teléfono: 964461668 y 953460669

2.1.2. El/La operador/a de soporte técnico de mesa de ayuda es el responsable de registrar y clasificar los requerimientos e incidentes a nivel microinformático solicitados por los usuarios del OEFA, a través del Aplicativo de Mesa de Ayuda. Luego del registro procede a realizar la asignación al personal de soporte técnico.

2.1.3. El/La operador/a de soporte técnico luego de realizar los descartes según sea el caso y resolver los requerimientos e incidentes, cierra el ticket de atención. De lo contrario deberá derivar hacia los especialistas de la OTI. El/la especialista de la OTI ejecuta las acciones necesarias para solucionar el incidente o requerimiento, así como documentar la solución según el I-OTI-PA0303-2 Instructivo de atención de solicitud de servicio de TI. En caso la solicitud o incidente no pueda ser resuelto, se derivará hacia un proveedor de servicio.

2.1.4. El/La operador/a de soporte técnico detecta que hay un conjunto de incidentes reportados por usuarios, se considera la atención como un problema y comunica al Gestor/a de Soporte Técnico para dar la prioridad de atención y remitir a los especialistas de la OTI o a proveedores de servicio para su atención y cierre.

2.2. Eventos[1] e incidentes[2] de seguridad de información

2.2.1. Primer nivel - El/la operador/a de soporte técnico de mesa de ayuda es el responsable de registrar y clasificar (ver Anexo 1) los eventos e incidentes reportados de seguridad de información a través del aplicativo de mesa de ayuda. Para esto diagnostica y resuelve, de lo contrario deberá diagnosticar y resolver el equipo de segundo nivel. ***Ver las actividades del Instructivo I-OTI-PA0303-3 Gestión de incidentes de seguridad de información y ciberseguridad.***

2.2.2. Segundo nivel - El incidente de seguridad de la información según la clasificación establecida será atendido por el/la especialista de OTI según el tipo de componente al que corresponda (ver Anexo 2), y reportados hacia el Oficial de Seguridad y Confianza Digital mediante correo institucional, así como registrados y atendidos a través del aplicativo de mesa de ayuda según el catálogo de incidentes de seguridad.

El/La Oficial de Seguridad y Confianza Digital revisa el incidente y comunica al Equipo de Respuesta ante incidentes de seguridad digital para la respectiva atención, de acuerdo a cada rol. Asimismo, el/la gestor/a de incidentes de seguridad digital tiene la responsabilidad de verificar constantemente la Alerta Integrada de la PCM:
https://www.gob.pe/institucion/pcm/informes-publicaciones/467735-alerta-integrada-de-seguridad-digital-n-001-2020-pecert

En el caso que el incidente sea de Datos Personales

- El/la Oficial de Seguridad y Confianza Digital notifica a el/la responsable del tratamiento del Banco de Datos afectado, la resolución del incidente y el estatus en que se encuentra.
- El/La responsable del Banco de Datos Personales, en coordinación con el/la Oficial de Seguridad y Confianza Digital revisan las consecuencias legales que el incidente podría ocasionar a la Institución y comunican en el día de ocurrido el incidente, mediante correo institucional a el/la Oficial de Datos Personales.
- Posterior a ello se realiza el seguimiento de las acciones a tomar o se cierra el ticket de atención.

[1] Ocurrencia identificada de un sistema o servicio que determine una posible infracción de los compromisos de Seguridad de la Información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad de información.

[2] Incidente de seguridad de información: Uno o una serie de eventos de seguridad de la información no deseados o inesperados que tiene una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información

2.2.3. El especialista de la OTI, realiza el análisis y descarte correspondiente para dar una solución definitiva.
- En caso de incidente de SI, el especialista de OTI diagnostica y da solución al mismo y utiliza el Diagrama causa-efecto/ Ishikawa como evidencia del análisis.

2.2.4. En el caso que el especialista de la OTI no logre resolver el incidente, este será escalado hacia el fabricante o proveedor, según corresponda.

2.2.5. Tercer nivel - Si el resolutor final fuera el fabricante o proveedor, se adjuntará el informe de la solución como parte de la evidencia necesaria para la gestión del proceso.

2.3. En relación a las debilidades[3]

- Los/Las usuarios/as y contratistas que usan los sistemas y servicios de información de la Entidad son advertidos de reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios a través de las concientizaciones o capacitaciones que se canalizan por la mesa de ayuda, con los siguientes contactos: soporte@oefa.gob.pe y números de teléfono: 964461668 y 953460669 en el cual se brindará la atención correspondiente.

- Las debilidades de seguridad de información serán canalizadas a través de la mesa de ayuda de OEFA para lo reportado por los/las usuarios/as o contratistas y adicionalmente las debilidades que pudiera identificar el Oficial de seguridad y confianza digital en las inspecciones programadas a lo largo del año (Acta de debilidades).

2.4. Aprendizaje de los incidentes

- El conocimiento adquirido a partir del análisis y resolución de los incidentes de seguridad de información permitirá identificar los incidentes recurrentes o de alto impacto o la necesidad de mejorar o agregar controles limitando las futuras ocurrencias. Asimismo, serán utilizados con el debido cuidado de confidencialidad como ejemplos de lo que podría suceder, cómo responder a los incidentes y cómo evitarlos en el futuro.

2.5. Recolección de evidencia

El/La Oficial de seguridad y confianza digital coordina con el Equipo de respuesta ante incidentes de seguridad digital, quienes de acuerdo a su rol se encargan de realizar: la investigación del incidente, recopilación de evidencia, conservación y análisis. Cabe mencionar, que las actividades del Equipo de Respuesta ante incidentes se encuentran descritas en la Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital de la PCM.

[3] Debilidad: es un defecto o vulnerabilidad sobre un activo o un control de información que puede dejarlo expuesto ante una amenaza.

https://www.gob.pe/institucion/pcm/informes-publicaciones/2986553-guia-para-la-conformacion-e-implementacion-de-equipos-de-respuestas-ante-incidentes-de-seguridad-digital

La investigación del incidente se encontrará a cargo del Gestor de Incidentes del OEFA (rol asignado de acuerdo al equipo de respuesta ante incidentes) para las acciones correspondientes, si se llega a identificar que el/la usuario/a fue responsable de generar el incidente, se comunicará a su jefe/a o coordinador/a para las acciones pertinentes dentro del marco legal vigente.

La recopilación de la información se desarrolla de la siguiente manera:

a. Evaluar las acciones realizadas por el personal involucrado en el momento del incidente.

b. Si el incidente involucra componentes físicos, se analizarán los equipos afectados y las posibles fallas que pudieron tener; así también se verificarán últimos mantenimientos realizados.

c. Solicitar a los/las servidores civiles que no usen los equipos informáticos involucrados lo antes posible y no permitir que vuelvan a utilizarlos hasta que se haya solucionado el incidente y se conozca la causa. Para el caso de equipos de terceros, se identifica al personal informático interno (administradores de sistemas, programadores, y otros) y/o a los usuarios de aplicaciones específicas para someterlos al peritaje. Identificar al dueño o usuarios del equipamiento informático, lo cual será de utilidad para la pericia.

d. Fotografiar los equipos informáticos involucrados antes de moverlos o desconectarlos. Realizar una toma fotográfica completa del lugar donde se encuentren los equipos informáticos involucrados, y fotos de las pantallas de las computadoras, si están encendidas.

e. En caso aplique, se considerará no tocar el material informático sin uso de guantes descartables. Dependiendo el objeto de la investigación, el teclado, monitores, mouse, y otros; que podrán ser utilizados para el análisis de huellas dactilares.

f. Si los equipos están apagados deben quedar apagados, si están encendidos deben quedar del mismo modo y consultar con el especialista técnico a cargo la modalidad de apagado.

g. Identificar si existen equipos conectados a una línea telefónica, y de ser el caso precisar el número telefónico para registrarlo en el acta de allanamiento.

h. Impedir que alguien realice búsquedas sobre directorios o intente ver la información almacenada en los dispositivos para evitar la posibilidad que se altere y destruya evidencia digital (esto incluye intentar hacer

una *"copia"* sin tener software forense específico y sin que quede documentado en el expediente judicial el procedimiento realizado).

i. Identificar correctamente todo el material tecnológico a aislar:

- Aislar únicamente los dispositivos informáticos que almacenan grandes volúmenes de información digital (PC´s, laptops y discos duros externos).

- Rotular o etiquetar el hardware que se va a aislar con los siguientes datos: N° de Expediente, Fecha y Hora, Número de Serie, Fabricante, Modelo; según corresponda.

i. Utilizar bolsas especiales antiestáticas para almacenar discos duros y otros dispositivos de almacenamiento magnético (si no se cuenta, se podrá utilizar bolsas de papel madera). Evitar el uso de bolsas plásticas, éstas podrían causar una descarga de electricidad estática que puede destruir los datos.

j. Colocar precinto en cada equipo informático, en todas sus entradas eléctricas y todas las partes que puedan ser abiertas o removidas. En caso de requerirse el traslado de las evidencias, el personal a cargo del transporte tiene la responsabilidad de evitar daños y alteraciones de todo el material informático hasta que sea peritado. Asegura la integridad de la evidencia digital verificando que los precintos estén completos al momento de ser entregado, para las prácticas forenses por profesionales calificados.

Anexo 1

Categoría	Causas	Clasificación Evento / Incidente
Evento o Incidente SI	● Incumplimientos de políticas, normas y/o procedimientos del Sistema de seguridad de la Información. ● Cambios no controlados en los sistemas (software y hardware) y servicios. ● Fallas en software y/o hardware. ● Violaciones de acceso a los sistemas. ● Ataques por software de tipo malicioso (malware). ● Correos fraudulentos (phishing). solicitando información del usuario. ● Pérdida o fuga de Información. ● Mal uso y abuso del correo electrónico. ● Detección de vulnerabilidades de seguridad. ● Afectación de banco de datos personales.	Se clasificará en evento o Incidente de Seguridad de información si cumple las siguientes condiciones: Evento SI: Si cumple con alguna de las causas definidas y ha vulnerado un control establecido, podría afectar uno o varios procesos y/o uno de los pilares de la SI, pero su nivel de afectación no interrumpe las operaciones. Incidente SI: Si cumple con algunas de estas causas definidas, y ha vulnerado un control establecido y está afectando uno o varios procesos y/o uno de los pilares de la SI, y su nivel de afectación interrumpe las operaciones.

Anexo 2

TIPO DE COMPONENTES	APLICACIONES Y RECURSOS CRÍTICOS
Energía	Transformador de aislamiento Equipo de suministro eléctrico para servidores y equipos de comunicaciones
	Aire acondicionado de precisión para el Centro de Datos
	UPS: Equipo de suministro eléctrico para servidores y equipos de comunicaciones
Appliance	Seguridad Perimetral firewall
Comunicaciones	Switches core y switch de distribución
	switches de acceso (piso)
	Internet activo confirmado por el proveedor
Sistema de almacenamiento	Storage
Servidores físicos	Servidor Blade, Servidor Base de datos Oracle y Servidor de Directorio principal
Servidores críticos virtuales	Servidor de dominio secundario (Directorio Activo)
	Gestor documental Alfresco: Repositorio de Información
Servidores Complementarios virtuales	Aplicaciones: JBOSS EAP, JBOSS FUSE, TOMCAT y Apache (servidores Linux)
	Administración de Servicios: Servidor de monitoreo de software y hardware
	Servidor de monitoreo de base de datos (Oracle Cloud Control) - Linux
	Base de Datos SQL Server.
	Sistemas operativos: Windows, Linux (otros servicios)
	Seguridad: Antivirus Kaspersky
	Servidor del portal web institucional.
	Servidor de Fuentes: Repositorio de Información
Appliance	Servidor de Telefonía IP y servidor físico de Telefonía IP
	Servidor de backups donde se encuentra instalado el software de respaldo, para las copias y restauración de información(disco)
Librería de backups	Equipo donde se realizan las copias de respaldo en medios magnéticos, y es utilizado para la restauración de información (cinta).

Instructivo de atención de solicitud de servicio de TI

I. OBJETIVO

Establecer las tareas para la atención de los servicios de TI a nivel del registro de solicitudes de servicio y control de inventarios de software y hardware.

II. INSTRUCCIONES

2.1 Consideraciones

- El inventario de software y hardware es el registro general de la información sobre las características, condiciones y ubicación del software y hardware en el Organismo de Evaluación y Fiscalización Ambiental - OEFA, el cual es administrado y actualizado por el/la Supervisor/a de Soporte Técnico utilizando el Aplicativo de Mesa de Ayuda.

- La actualización del inventario de software y hardware puede ser: *(i)* total; cuando se realiza con una frecuencia anual; o, *(ii)* parcial; cuando se realiza atendiendo a la incorporación, adquisición, movimientos y bajas de hardware y software, cuando se requiera.

- El registro de inventario de software y hardware comprende los siguientes: los equipos informáticos, servidores tecnológicos y equipos de comunicaciones en uso y aquellos que no estando en uso se encuentren asignados o almacenados en las áreas del OEFA.

2.2 Sobre el hardware

- La OTI evaluará periódicamente los recursos informáticos, en cuanto a cantidad, calidad, requerimientos y estado de conservación, a fin de racionalizar y optimizar el uso de los mismos atendiendo a las necesidades reales del usuario en correspondencia con el equipo asignado y determinar si éste es adecuado para realizar las actividades encomendadas. Las distintas áreas del OEFA son responsables de brindar el apoyo y facilidades para este propósito, en el marco de sus funciones.

- Los Jefes/as o Directores/as coordinan con la OTI la asignación de equipos, según disponibilidad.

- Las impresoras deben ser administradas por el equipo de soporte técnico y utilizadas racionalmente a fin de no generar gastos innecesarios y maximizar la eficiencia del equipo. Se debe priorizar la documentación electrónica e imprimir solo cuando sea necesario. Las impresoras se instalarán en red para optimizar su uso por múltiples usuarios/as, y todas cuentan con una unidad Dúplex, con la finalidad de imprimir por ambas caras de la hoja, maximizando el uso del papel.

- La OTI y la Oficina de Administración, en el marco de sus funciones, coordinan a efectos de desarrollar las acciones necesarias para brindar el mantenimiento preventivo y/o correctivo de los equipos informáticos, de manera que se garantice su disponibilidad de manera ininterrumpida. Se considera que el mantenimiento preventivo y correctivo es realizado por los contratistas durante la vigencia del periodo de garantía de los equipos de cómputo establecido en sus contratos, culminado el periodo de garantía corresponde al equipo de soporte técnico de la OTI del mantenimiento preventivo y correctivo.

- Los/Las usuarios/as de la Entidad no debe reparar o permitir que se repare un equipo informático por personal no acreditado por la OTI.

2.3 Sobre el software

- Toda adquisición de software que realice el OEFA se sujeta a lo dispuesto en la Ley N° 28612 - Ley que Norma el Uso, Adquisición y Adecuación del Software en la Administración Pública y su Reglamento, aprobado por el Decreto Supremo N° 024-2006-PCM, priorizando el uso de software libre.

- Los/Las usuarios/as del OEFA no deben instalar software sin autorización de la OTI, en los equipos informáticos y celulares asignados por el OEFA. Todo requerimiento deberá ser coordinado con la OTI, previa verificación de la existencia de licencias previamente adquiridas.

2.4 Requerimientos de hardware

- Los/Las usuarios/as o servidores/as civiles del OEFA que, por necesidades del servicio, requieran equipos informáticos como computadoras, impresoras, escáner u otros similares, deben solicitarlo sustentando su necesidad a través de su Jefe/a o Director/a mediante memorando dirigido a la OTI.

- La OTI remite las especificaciones técnicas y el requerimiento de compra respectivo a la Unidad de Abastecimiento de la Oficina de Administración.

- La OTI es responsable de recibir, evaluar, autorizar y tramitar los requerimientos de adquisiciones de hardware y software de cualquier índole en el OEFA.

- La OTI se encarga de que todos los soportes de almacenamiento de datos sean comprobados para confirmar que todo dato sensible y software bajo licencia se ha eliminado de manera segura, antes de deshacerse de ellos o reutilizarse.

- La Unidad de Abastecimiento de la Oficina de Administración mantiene el registro de los dispositivos móviles asignados a los/as usuarios/as mediante un acta de entrega. Si el dispositivo móvil se devuelve a la empresa proveedora de servicio una vez terminado el contrato, la OTI realiza la restauración de fábrica para eliminar información del usuario que

haya quedado en el dispositivo móvil. Asimismo, se debe considerar lo descrito en el procedimiento PA0211 *"Actos de gestión patrimonial de los bienes muebles de propiedad del OEFA"*.

2.5 Sobre la responsabilidad de los/las usuarios/as y la seguridad de la información

- El acceso a los aplicativos está restringido sólo a sus usuarios/as, los cuales no deben compartir sus claves de acceso con terceras personas.

- Los/as Usuarios/as son responsables de las siguientes acciones:

  a) Actualizar sus claves de acceso periódicamente, manteniendo la confidencialidad y el nivel de complejidad de la clave.

  b) No utilizar medios extraíbles (USB, discos externos, etc.) provenientes del exterior del OEFA, sin antes ser verificados con el antivirus oficial determinado por la OTI.

  c) No difundir, a través de páginas web, correo personal o correo institucional, información, documentos confidenciales, claves o datos que puedan afectar la seguridad del OEFA. El/La Directora/a o Jefe/a de la Oficina es responsable de la información a su cargo, por lo que debe hacer cumplir las actividades mencionadas precedentemente.

  d) No abrir el correo de remitentes desconocidos o respecto del cual se tenga dudas sobre su identidad, así como descargar o ejecutar cualquier archivo adjunto, debido a que se corre el riesgo que contenga algún virus.

  e) Evitar la ejecución de archivos externos con extensiones tales como: exe, com, gif, dll, debido a que contienen virus o programas maliciosos. Aún si se tuviera confianza en el remitente, existe la probabilidad de que también esté infectado.

  f) No instalar aplicaciones/software de ningún tipo, incluso aquellos que se requieran licencias y que no sean autorizados expresamente por la OTI, de lo contrario, el/la usuario/a es responsable de las consecuencias legales o sanciones correspondientes. El/La Director/a o Jefe/a del área usuaria vela por el cumplimiento de esta disposición.

  g) Los/as usuarios/as deben eliminar permanentemente de su disco duro la información duplicada o aquellos archivos que no volverán a ser utilizados, teniendo en cuenta que es un medio de almacenamiento temporal de información.

2.6 Protección de los equipos y mantenimiento por el/la usuario/a

- Los/Las usuarios/as son responsables de brindar atenciones preventivas básicas a su PC u otro equipo asignado, tales como: limpieza externa con paño seco, mantener su equipo en ubicación adecuada para evitar caídas.

- Los/Las usuarios/as o servidores/ras no deben comer, beber o fumar cerca de los equipos de cómputo, a fin de conservarlos en óptimo estado.

- El uso de las impresoras, grabadoras de CD y cualquier otro recurso informático de propiedad del OEFA, debe estar relacionado únicamente a los fines institucionales, conforme a lo dispuesto en el Literal t) del Artículo 48 del Reglamento Interno de los Servidores Civiles[1].

- Los/Las usuarios/as no deben manipular los equipos informáticos (abrirlos, cambiar dispositivos, etc.). El/La Director/a o Jefe/a es el/la responsable final del equipo asignado a los/as usuarios/as a su cargo, por lo que debe hacer cumplir las actividades mencionadas precedentemente.

- No se debe movilizar y/o intercambiar equipos y sus componentes con equipos de otras áreas sin conocimiento previo del responsable de Control Patrimonial de la Unidad de Abastecimiento ***de la Oficina de Administración*** y de la OTI, a fin de que se evalúe y tramite el pedido. El/La Director/a o Jefe/a del área usuaria debe hacer cumplir las actividades precedentemente. Si los equipos fueron identificados por la OTI como activos de información, la movilización de estos equipos debe ser autorizados por el/la Director/a o Jefe/a o responsable de dicho activo.

- Los/Las usuarios/as deben informar a la OTI cuando detecte una ubicación inadecuada del cableado o componentes de red, por ejemplo: la superposición con cableados eléctricos o telefónicos, debido a que éstos pueden causar interferencias en la conectividad.

- Los/Las usuarios/as son responsables de encender y apagar correctamente todos los componentes de su PC.

- ***En caso se realice el teletrabajo y la Entidad disponga de equipos para el préstamo, el/la usuario/a debe solicitar la debida autorización al área de Control Patrimonial y gestionar su traslado. Por lo que el área de Control Patrimonial durante la movilización y/o traslado de los equipos debe tomar las medidas adecuadas para evitar la pérdida, extravío, daño, robo u olvido de los mismos, así como el acceso indebido por parte de personal no autorizado.***

[1] Aprobado mediante la Resolución de Gerencia General N° 019-019-OEFA-GEG.

2.7 Sobre uso de internet

- El uso de Internet está relacionado únicamente a los fines institucionales y está sujeto a supervisión por parte del equipo de infraestructura y comunicaciones de la OTI.

- El/La responsable de la administración de la red realiza las evaluaciones periódicas sobre lo siguiente: *(i)* las cuentas de los/as usuarios/as, para verificar que el de uso de Internet esté relacionado a los fines dispuestos por la Entidad[2]; *(ii)* la racionalización y optimización del tráfico en la red.

2.8 Sobre el uso de dispositivos o medios extraíbles USB

- Los/Las usuarios/as que requieran usar dispositivos USB deben contar con la autorización de el/la Director/a o Jefe/a del área usuaria y verificar que los mismos no contengan virus, por lo cual deben cumplir con lo siguiente:

  a) Verificar que su equipo de cómputo tenga instalado el software antivirus actualizado con la última firma de virus del día.

  b) Insertar el dispositivo USB y realizar un escaneo de virus, con la finalidad de encontrar y/o eliminar algún programa malicioso alojado en dicho dispositivo.

  c) Solo si el dispositivo USB está libre de virus puede ser usado, de lo contrario debe coordinar con personal de soporte técnico de la OTI; a efectos de eliminar el virus detectado.

2.9 Sobre seguridad de datos

- La OTI es responsable del mantenimiento de la red informática del OEFA, de nuevas conexiones, del tráfico y cableado estructurado, asimismo el/la especialista en aplicaciones y telecomunicaciones ejecuta las siguientes actividades:

  a) Instalar, configurar, operar y administrar los Servidores de la Red del OEFA;
  b) Ejecutar los controles indicados en las políticas de seguridad de la información relacionadas a la red informática del OEFA.
  c) Instalar y dar mantenimiento a los sistemas de alarmas y video vigilancia, los cuales se encuentran integrados a la red informática del OEFA.

- El/La administrador/a de base de datos establece las normas de acceso restringido a los sistemas, bases de datos y servidores informáticos del OEFA, a fin de salvaguardar la información.

[2] Precisar que la OTI desarrolla un seguimiento respecto a los/as usuarios/as que hagan uso indebido del Servicio de Internet y que descarguen archivos no relacionados con el servicio prestado para el OEFA.

- El/La Analista de redes genera las copias de respaldo (backups) de la información de los servidores/as civiles del OEFA a través de medios magnéticos u ópticos (cintas, discos removibles o similares), las cuales se mantienen bajo custodia del contratista según lo establecido en los términos contractuales. Dichas copias deben tener etiquetas con el nombre de las aplicaciones, nombres de archivos o información que contiene el backup, detalle del formato de compresión, cintas magnéticas; asimismo, las etiquetas también deben contener la versión y fecha de proceso de respaldo.

- Instalar y desinstalar el software autorizado para los/as usuarios/as, a fin de regular el adecuado uso de los equipos, evitando problemas legales y el mal funcionamiento del mismo.

- Establecer las acciones de seguridad en Internet contra terceros, mediante la implementación de un servidor Firewall, así como, disponer las claves de acceso (password) para los programas desarrollados y establecer los niveles de acceso a la información, como consulta, actualización, administración.

2.10 Sobre actualización de antivirus

- Las actualizaciones del antivirus en las computadoras se realizan automáticamente desde un servidor de la red del OEFA y son verificadas por el/la Analista de redes. ***Cabe mencionar que el servicio de antivirus lo brinda el contratista para las estaciones de trabajo (computadoras personales, laptops) y servidores (físicos y virtualizados) de la red del OEFA. Este servicio debe considerar las siguientes actividades:***

  - ✓ ***Permite la instalación remota de aplicaciones en equipos cliente.***
  - ✓ ***Actualiza las bases de datos y los módulos del antivirus.***
  - ✓ ***Permite controlar las directivas y las tareas de grupo en equipos cliente.***
  - ✓ ***Almacena información sobre eventos de los equipos.***
  - ✓ ***Crea reportes sobre el funcionamiento de las aplicaciones.***
  - ✓ ***Distribuye la licencia en los equipos cliente y almacena la información sobre su uso.***
  - ✓ ***Envía notificaciones sobre las tareas que se ejecutan en equipos cliente. Por ejemplo, las notificaciones pueden informar sobre virus detectados en equipos cliente.***

- ***Medidas inmediatas para eliminar el malware el cual es realizado por el equipo de soporte técnico previa comunicación de el/la usuario/a:***
  a) Desconéctese del internet para impedir que el malware cause más daños
  b) Reinicie su computadora en "Modo Seguro"

c) Elimine los archivos temporales con la herramienta "Liberador de espacio en disco"
d) Ejecute el análisis a petición en el "Antivirus" que tenga la Entidad, y seguir las instrucciones que indique dicho producto.
e) Si detecta malware, elimine el archivo o póngalo en cuarentena.
f) Reinicie su computadora o laptop.
g) Cambie las contraseñas si cree que se han filtrado.
h) Actualice el software, el navegador y el sistema operativo.
i) Vuelva a analizar la computadora para comprobar que no haya más amenazas.

- El/La Analista de redes verifica que el servidor se actualice permanentemente y que brinde el servicio de actualización a las computadoras del OEFA. Es responsabilidad de los/as usuarios/as verificar que el antivirus se encuentre actualizado y ante cualquier problema o consulta comunicarse con la Mesa de Ayuda de la OTI.

2.11 Sobre copia de respaldo o backup de carpeta de usuario

- La copia de respaldo o backup de la respectiva carpeta de cada usuario/a del OEFA, debe ser almacenada en un servidor informático de archivos a cargo de la OTI. Además, debe realizarse copias en medios magnéticos (CD, DVD, Discos Externos o similares) debidamente identificados mediante etiquetas.

2.12 Sobre el uso del correo institucional

- El correo institucional es el sistema de correo personal que los/as usuarios/as de la red del OEFA emplean como medio de envío y recepción de información.

- La OTI es responsable de brindar el mantenimiento adecuado, asignar racionalmente las cuentas institucionales, así como supervisar el uso del correo institucional.

- Los/Las usuarios/as cuentan con cuentas asignadas en el sistema de correo institucional, como única dirección electrónica, con clave de acceso, cuya custodia e inviolabilidad será de su responsabilidad, no pudiendo por ningún motivo entregar su clave a otra persona.

- La clave de acceso debe ser de una longitud de no menos de ocho caracteres de preferencia mayúsculas y minúsculas, adicionalmente puede incluir caracteres especiales.

- La OTI puede suspender temporal o definitivamente las cuentas de correo electrónico institucional de un/a usuario/a, previo aviso y de acuerdo a las disposiciones de la Alta Dirección.

2.13 Atenciones de servicio

- El personal que conforma el CAU[3] es el único autorizado para brindar el servicio de soporte técnico. El/La usuario/a no debe permitir que personal no autorizado manipule el recurso informático asignado, bajo responsabilidad.

- Para la atención del servicio de soporte técnico, el CAU cuenta con las siguientes modalidades: *(i)* correo institucional: soporte@oefa.gob.pe; y, *(ii)* medio telefónico: Aló OTI Anexo 6000.

- El CAU cuenta con un registro de atención de las solicitudes de soporte técnico que debe contener, como mínimo, la siguiente información:

  a) Datos de el/la usuario/a: Nombres y Apellidos, área y correo institucional.
  b) Datos del recurso informático: Tipo de recurso y en el caso de equipos informáticos, adicionalmente, el código patrimonial.
  c) Descripción del incidente o asistencia: Tipo de falla o de requerimiento, diagnóstico preliminar, entre otra información relevante.
  d) Datos de la atención brindada: Fecha y hora de inicio y término de la atención, nombre del técnico de soporte que brindó la atención, estado y solución.

2.14 Requerimiento de cuentas de usuario de red y cuentas de correo institucional

- Para la creación de las cuentas de usuario de red y cuentas de correo electrónico se debe considerar lo siguiente:

Creación de usuarios/as de red	Creación de correo institucional
• Servidor/a Civil • Secigristas • Practicante pre profesional • Practicante profesional • Terceros • Locadores	• Servidor/a Civil • Secigristas • Practicante pre profesional • Practicante profesional • Locadores

  a) La atención se inicia con el registro del requerimiento mediante correo institucional o llamada telefónica, por parte del área usuaria, en los siguientes casos:

[3] El Centro de Atención al Usuario (CAU), se encuentra conformado por los técnicos de soporte, operador de soporte técnico y liderado por el/la supervisor/a de soporte técnico.

- Para el caso de locadores/as se debe adjuntar la orden de servicio para tener en cuenta el periodo de contrato y se registra el Anexo N° 01 *"Formato de alta y baja de usuarios/as"*. En la solicitud se debe indicar si el acceso también corresponde al banco de datos personales de la Entidad, el mismo que es probado por el/la Responsable del tratamiento de banco de datos personales.

- ***Para el personal bajo el régimen de Contratación Administrativa de Servicios (en adelante, CAS) o Contratación bajo el Régimen Servir,*** la Unidad de Gestión de Recursos Humanos de la Oficina de Administración ***debe*** ingresa**r** el requerimiento por medio del Sistema Integrado de Administración (SIA-RRHH), ***en base a ello la OTI realiza el Alta de usuario. Asimismo, cuando un personal se desvincula, la Unidad de Gestión de Recursos Humanos de la Oficina de Administración remite el requerimiento a la OTI mediante el SIA-RRHH para la baja de usuarios y sus respectivos accesos a red y a las aplicaciones. Asimismo, cuando un personal del OEFA pide licencia sin goce de haber, la URH debe comunicar a la OTI para suspender sus accesos hasta la fecha que retornaría el personal.***

b) El/La operador/a de soporte técnico valida si el requerimiento contiene la información necesaria para que pueda ser atendido adecuadamente, considerando los siguiente:

- Para el caso del personal bajo el régimen CAS o Contratación bajo el Régimen Servir verificar que se adjuntó al correo institucional del requerimiento por parte de la Unidad de Gestión de Recursos Humanos de la Oficina de Administración.

- Para el caso de locadores/as la información señalada en el Literal a) del presente instructivo.

- En caso el requerimiento no contenga la información necesaria, el/la Operador/a de soporte técnico comunica mediante correo institucional, al área usuaria solicitante para actualizar la información.

c) La creación de cuentas de correos institucionales genéricas, es decir, no asociadas a un/a usuario/a, se realizará en los siguientes supuestos:

i. Para la creación de cuentas de correo electrónico, el área usuaria solicita en virtud de una normativa interna o un rol de trabajo específico dentro del OEFA, en el cual se debe indicar la normativa que sustenta la creación de la referida cuenta adjuntando dicha resolución u otro documento que lo designe. Ejemplos de este supuesto son: oficial-antisoborno@oefa.gob.pe, protegemostusdatos@oefa.gob.pe, entre otros.

ii. Para la creación de cuentas en virtud a los servicios de plataformas informáticas, se debe indicar cuál es el sistema o aplicativo

informático que requiere la creación de la cuenta de correo, esta solicitud la realiza el área usuaria. Ejemplos de este supuesto son: denuncias@oefa.gob.pe, sinada_web@oefa.gob.pe, entre otros.

iii. Otros: Aquí se debe sustentar la creación de la cuenta de correo electrónico genérico. Solo en este caso, es necesario la autorización de la Gerencia General.

- Una vez finalizada la validación del requerimiento de cuentas, es derivada para su atención al área de infraestructura y comunicaciones, de acuerdo al Instructivo I-OTI-PA0304-1 *"Mantenimiento de Base de datos"*.

- El área de infraestructura y comunicaciones de la OTI es el resultado de la atención al área de soporte técnico para que las cuentas de usuario de red y correo electrónico sean configuradas a los/as usuarios/as finales.

- El/La operador/a de soporte técnico comunica por correo institucional a el/la asistente administrativo del área usuaria indicando el/la usuario/a y correo institucional con las claves genéricas para el primer ingreso del personal nuevo.

- Al finalizar la atención del requerimiento, se envía de manera automática a el/la usuario/a solicitante una encuesta de satisfacción mediante el Aplicativo de mesa de ayuda para medir su satisfacción general con el servicio proporcionado.

2.15 Instalación de software

Los requerimientos de instalación de software deben ser solicitados mediante correo institucional o llamada telefónica, conforme a los siguientes criterios:

a) La atención se inicia con el registro del requerimiento mediante el aplicativo de mesa de ayuda por parte de el/la usuaria.

b) El/La operador/a de soporte técnico valida si el requerimiento contiene la información necesaria para que pueda ser atendido adecuadamente, considerando los siguiente:

- El nombre del software requerido.
- Tipo de Software (Libre / Licenciado).
- Nombre del equipo para realizar la instalación de manera remota.

c) Si el software es licenciado, el área de soporte técnico verifica si se cuenta con disponibilidad de licencias.

d) Si el software es libre, se procede con la instalación correspondiente.

e) Una vez validado el requerimiento, el mismo puede ser derivado para su atención al área de soporte técnico, en caso contrario se informa a el/la usuario/a sobre el motivo por el cual no podrá ser atendido su requerimiento.

f) Al finalizar la atención del requerimiento sea en primer, segundo o tercer nivel el Aplicativo de Mesa de Ayuda remite, mediante correo institucional, a el/la usuario/a una encuesta de satisfacción para medir su satisfacción general con el servicio proporcionado.

2.16 Registro de software instalado

- El registro de software instalado se inicia cuando un equipo informático está conectado a la red institucional, detectando sus características técnicas con todo el software instalado en el mismo.

2.17 Registro de licencia de software

- El registro de licencia de software se realiza utilizando la solución de gestión de servicios de tecnologías de la información, en la cual se registra la información obtenida de los contratos de licencias de software y la cantidad de las mismas, las cuales serán posteriormente administradas por la OTI y Control Patrimonial.

2.18 Inventario de hardware y software

- El inventario de hardware y software es realizado utilizando la solución de gestión de servicios de tecnologías de la información y se realiza de la siguiente manera:
  a) El registro de los activos de hardware y software se realiza cuando un equipo informático es conectado a la red institucional. Automáticamente el aplicativo de servicios de tecnologías de la información detecta al equipo informático y sus características técnicas junto con todo el software instalado en el mismo, manteniendo un inventario actualizado de hardware y software.

  b) Luego de tener la información captada por el sistema se realiza un cruce con la información de la Oficina de Control Patrimonial para obtener los Códigos Patrimoniales según el número de serie obtenido por la solución de gestión de servicios de tecnologías de la información.

2.19 Reporte de incidente o solicitud de asistencia (software)

- Los reportes de incidente o solicitud de asistencia de software son ingresados mediante correo institucional o llamada telefónica, considerando lo siguiente:

a) La atención se inicia con el registro del requerimiento mediante correo institucional o llamada telefónica por parte de el/la usuario/a y/o el/la operador/a de soporte técnico.

b) El/La operador/a de soporte técnico valida si el requerimiento contiene la información necesaria para que pueda ser atendido en primer nivel, en caso el requerimiento no pueda ser atendido se escalará a segundo o tercer nivel para su atención correspondiente.

c) Una vez escalado el requerimiento, su atención es realizada vía telefónica, por correo institucional, de manera remota o de manera presencial cuando resulte técnicamente pertinente.

d) Al finalizar la atención del requerimiento sea en primer, segundo o tercer nivel el Aplicativo de Mesa de Ayuda remite, mediante correo institucional, a el/la usuario/a una encuesta de satisfacción para medir su satisfacción general con el servicio proporcionado.

2.20 Reporte de incidente o solicitud de asistencia (hardware)

- Los requerimientos de incidente o solicitud de asistencia de hardware son ingresados mediante correo institucional o llamada telefónica y se realiza de la siguiente manera:

  a) La atención se inicia con el registro del requerimiento mediante correo institucional, o llamada telefónica por parte de el/la usuario/a y/o el/la operador/a de soporte técnico.

  b) En primera instancia el/la operador/a de soporte técnico realiza el diagnóstico previo de los equipos para verificar si se trata de un inconveniente que puede ser resuelto de forma telefónica.

  c) En caso el incidente o solicitud no pueda ser resuelto en primera instancia y se trate de casos de conectividad de red o que los equipos no estén encendiendo o respondiendo, los mismos serán derivados para la atención in situ.

  d) En caso de que el equipo tenga que ser reparado, el/la operador/a de soporte técnico coordina con el/la usuario/a para el repliegue del equipo y a la vez procederá con el proceso de garantía. En caso que el equipo no cuente con garantía el/la operador/a de soporte técnico coordina con el/la usuario/a la sustitución del equipo.

  e) Al finalizar la atención del requerimiento sea en primer, segundo o tercer nivel el Aplicativo de Mesa de Ayuda remite, mediante correo institucional, a el/la usuario/a una encuesta de satisfacción general con el servicio proporcionado.

2.21 Registro de hardware

- El registro de hardware es realizado mediante la solución de gestión de servicios de tecnologías de la información, iniciando y culminando cuando un equipo informático está conectado a la red institucional y automáticamente se detecta al equipo informático y sus características técnicas.

2.22 Requerimiento de equipos y/o componentes

- El requerimiento de equipos y/o componentes se ingresa a través del correo institucional, memorando y se realiza de la siguiente manera:

  a) El/La Jefe/a o Director/a del área usuaria realiza la solicitud del equipo o componente requerido mediante correo institucional o llamada telefónica.
  b) El/La operador/a de soporte técnico deriva el requerimiento al supervisor/a de soporte técnico para la gestión y atención del requerimiento considerando la disponibilidad de equipos y/o componentes.
  c) El/La operador/a de soporte técnico verifica si hay equipo disponible para entregar y de no contar con los equipos se coordinará con la Unidad de Abastecimiento de la Oficina de Administración (según presupuesto) la compra o alquiler de estos, según las necesidades del usuario.
  d) El/La operador/a de soporte técnico indica a el/la usuario/a el plazo de atención correspondiente.

2.23 Adquisición de licencias

- El/La Jefe/a o Director/a del área usuaria solicita mediante correo institucional o por memorando a el/la Jefe/a de la OTI a adquisición de licencias, y se realiza de la siguiente manera:

  a) La atención inicia con el registro de la necesidad de adquisición de licencias para un programa específico.
  b) El/La operador/a de soporte técnico deriva el requerimiento a el/la supervisor/a de soporte técnico para la gestión del requerimiento.
  c) El/La supervisor/a de soporte técnico realiza las acciones correspondientes para la atención del requerimiento, dentro de los cuales se encuentran:

     - La elaboración de los Términos de Referencia y/o Especificaciones Técnicas.
     - El Informe Técnico Previo de Evaluación de Software (Anexo N° 02 *"Formato Informe Técnico Previo de Evaluación")*.
     - El Informe de Estandarización, en caso sea necesario la adquisición de un software con nombre propio.

  d) Una vez adquirida la licencia se procede a comunicar, mediante correo institucional o memorando al área usuaria; a fin de realizar su instalación.

2.24 Eliminación de software

- La eliminación de software se solicita por medio de correo institucional o llamada telefónica, se realiza de la siguiente manera:

  a) La eliminación de software inicia cuando el/la usuario/a indica o identifica programas en su equipo de cómputo con los que no desea contar.

  b) El/La operador/a de soporte técnico valida si el requerimiento contiene la información necesaria para que pueda ser atendido, considerando lo siguiente:
  - Nombre de software.
  - Nombre del equipo para atender de manera remota.

  c) Una vez se cuente con la información necesaria, su atención es realizada vía telefónica o por correo institucional, de manera remota o de manera presencial cuando resulte técnicamente pertinente.

  d) Al finalizar la atención del requerimiento sea en primer, segundo o tercer nivel el Aplicativo de Mesa de Ayuda remite, mediante correo institucional, a el/la usuario/a una encuesta de satisfacción para medir su satisfacción general con el servicio proporcionado.

2.25 Instalación de software para firma digital

- Los requerimientos de instalación de software para firma digital deben ser solicitadas mediante correo institucional o llamada telefónica a la Mesa de Ayuda y se realiza de la siguiente manera:

  a) La atención se inicia con el registro del requerimiento mediante el aplicativo de mesa de ayuda por parte de el/la usuario/a final.

  b) El/La operador/a de soporte técnico valida si el requerimiento contiene la información necesaria para atender al usuario y deriva el requerimiento a el/la Técnico de Soporte para su atención correspondiente vía remota o de manera presencial.

  c) El/La operador/a de soporte realiza la lista de programas instalados para la verificación de los programas que faltan instalar; a efectos de que no existan problemas al momento de realizar la firma digital, dentro de dichos programas podemos mencionar los siguientes:

  - Java
  - Controlador de lector de DNI electrónico
  - SS***igner***

d) Finalizando la instalación del software para firma digital se realizan las pruebas de operatividad con el/la usuario/a para validar su conformidad.

e) Al finalizar la atención del requerimiento sea en primer, segundo o tercer nivel el Aplicativo de Mesa de Ayuda remite, mediante correo institucional, a el/la usuario/a una encuesta de satisfacción para medir su satisfacción general con el servicio proporcionado.

2.26 Instalación y configuración de equipos periféricos

- Todos los requerimientos instalación y configuración de equipos periféricos son ingresados mediante correo institucional o llamada telefónica, previa validación del el/la Jefe/a o Director/a del área usuaria, y se realiza de la siguiente manera:

a) La atención se inicia con el registro del requerimiento mediante correo institucional o llamada telefónica por parte de el/la usuario/a final y/o el/la operador/a de soporte técnico, previa validación por el/la Jefe/a o Director/a del área usuaria.

b) El/La operador/a de soporte técnico valida si el requerimiento contiene la siguiente información:

- Nombre de PC o laptop
- Número de anexo o equipo celular

c) De contar con toda la información necesaria y de tratarse de un caso de configuración, el/la operador/a de soporte técnico procede a realizar su atención en primer nivel, en caso de ser una instalación física la atención es realizada en segundo nivel por parte de un especialista de soporte técnico.

d) Al finalizar la atención del requerimiento sea en primer, segundo o tercer nivel el Aplicativo de Mesa de Ayuda remite, mediante correo institucional, a el/la usuario/a una encuesta de satisfacción para medir su satisfacción general con el servicio proporcionado.

2.27 Instalación y configuración de equipos multimedia

- Todos los requerimientos instalación y configuración de equipos multimedia se solicita, mediante correo institucional o llamada telefónica y se realiza de la siguiente manera:

a) La atención se inicia con el registro del requerimiento mediante correo institucional o llamada telefónica por parte de el/la usuario/a final y/o el/la operador/a de soporte técnico.

b) El/La operador/a de soporte técnico valida la información y escala el requerimiento a el/la técnico/a de soporte para la atención correspondiente, considerando la siguiente información:

- Ubicación
- Hora

c) Al finalizar la atención del requerimiento sea en primer, segundo o tercer nivel el Aplicativo de Mesa de Ayuda remite, mediante correo institucional, a el/la usuario/a una encuesta de satisfacción para medir su satisfacción general con el servicio proporcionado.

2.28 En relación a la constancia sobre los accesos a sistemas informáticos e información conexa vinculados a la entrega de cargo

- Cuando los/as servidores/as civiles realicen su entrega de cargo, deben solicitar a la OTI el Anexo N° 02*: "Formato de constancia sobre los sistemas informáticos e información conexa"* del *"Instructivo para la entrega y recepción de cargo del/la servidor/a civil del OEFA"* del Procedimiento PA0112 *"Desvinculación de los/las servidores/as civiles"*.

- En este contexto, las solicitudes de baja son ingresadas mediante correo institucional y se realiza de la siguiente manera:

a) La atención se inicia con el registro del requerimiento mediante correo institucional por parte de el/la usuario/a.

b) El/La operador/a de soporte técnico remite a el/la usuario/a, el enlace drive del formulario, a través del correo institucional; a fin de completar la siguiente información: *(i)* correo institucional, *(ii)* nombres y apellidos, *(iii)* área del OEFA, *(iv)* DNI, *(v)* nombre del puesto; y, *(vi)* motivo de la solicitud.

c) Una vez se cuente con toda la información requerida, el/la analista de mesa de ayuda asigna la atención a el/la operador/a de soporte técnico.

d) El/La operador/a de soporte técnico valida y completa el documento remitido por el/la usuario/a.

e) El/La operador/a de soporte técnico finaliza la atención enviando el anexo solicitado al correo del usuario.

f) Al finalizar la atención del requerimiento sea en primer, segundo o tercer nivel el Aplicativo de Mesa de Ayuda remite, mediante correo institucional, a el/la usuario/a una encuesta para medir su satisfacción general con el servicio proporcionado.

2.29 Respecto a los accesos para el teletrabajo

La OTI brinda accesos a los/as usuarios/as que tengan modalidad de teletrabajo de acuerdo a los equipos de cómputo que tienen:

a) Equipos de propiedad del OEFA

- Se realiza la coordinación entre el/la operador/a de soporte técnico con el/la usuario/a para que tenga acceso a la red de OEFA dependiendo de las actividades que van a realizar. En base a ello, se tiene las distintas herramientas a considerar por tipos de actividad:
  - ✓ VPN (propalms): se brinda a los/as usuarios/as que usen aplicativos que son cliente servidor (SIGA-OEFA cliente, SIARRHH Cliente), también al personal de la OTI que ingrese a servidores físicos o virtuales.
  - ✓ FTP: es una forma de acceder a los/as usuarios/as que tienen carpetas de red que están en un servidor del OEFA.
  - ✓ Teamviewer: es usado sólo por personal de la OTI.
  - ✓ Chrome remote desktop: se configura para cualquier usuario/a, se requiere que se encuentre de modo presencial para la configuración con el/la operador/a de soporte ya que debe colocar su usuario y contraseña.
- El/La operador/a de soporte técnico realiza la actualización del antivirus en el equipo.
- El/la operador/a de soporte técnico realiza la configuración y/o mantenimiento del equipo.

b) Equipos de propiedad del usuario

Se realiza la coordinación entre el/la operador/a de soporte técnico con el/la usuario/a para que tenga acceso a la red de OEFA dependiendo de las actividades que van a realizar. En base a ello, se tiene las distintas herramientas a considerar por tipos de actividad:

- ✓ VPN (propalms): se brinda a los/las usuarios/as que usen aplicativos que son cliente servidor ejemplo: SIGA-OEFA cliente, SIARRHH Cliente, también al personal de la OTI que ingrese a servidores físicos o virtuales.
- ✓ FTP: es una forma de acceder a los/las usuarios/as que tienen carpetas de red que están en un servidor del OEFA.

El/la operador/a de soporte técnico puede atender consultas de mantenimiento de los/las usuarios/as, sin embargo, no realizará configuraciones ni mantenimiento a dichos equipos. ***Cabe mencionar, que es responsabilidad de el/la usuario/a tener un antivirus actualizado en su PC o laptop cuando realice el teletrabajo, la OTI no se hace responsable de los equipos personales del colaborador.***

Anexo 01

Formato de alta y baja de usuarios/as

PERÚ | Ministerio del Ambiente | Organismo de Evaluación y Fiscalización Ambiental

Oficina de Tecnologías de la Información

Anexo 01
Versión: ***02***
Fecha: 26/05/2022

FORMATO ALTAS Y BAJAS DE USUARIOS CORREO ELECTRÓNICO Y RED
(Para ser llenado por Directores y/o Jefes de Oficina)

ALTA DE USUARIO	☐	ALTA TEMPORAL	☐
BAJA DE USUARIO	☐	BAJA TEMPORAL	☐

DATOS DE EL/LA USUARIO/A :

NOMBRE DE EL/LA USUARIO/A : _____

OFICINA / COORDINACIÓN: _____

MODALIDAD DE CONTRATACIÓN: PRACTICANTE ☐ SECIGRISTA ☐ LOCADOR ☐ TERCERO ☐

CONSIDERACIONES; Al personal Tercero/a solo se debe crear la cuenta de red

DAR ALTA O BAJA DE: FECHA DE SOLICITUD:

CORREO ☐

RED ☐

OFICINA SOLICITANTE : _____

DIRECTOR/A O JEFE/A DE UNIDAD _____

TELÉFONO DIRECTO : _____

FIRMA DIRECTOR/A O JEFE/A DE UNIDAD

(solo para ser llenado por la OTI)

ACCION REALIZADA :

ID USUARIO (RED) : _____

CORREO USUARIO : _____

FECHA : / /

RECOMENDACION : _____

NOMBRE DE EL/LA TÉCNICO/A (OTI) QUE ATIENDE : _____

JEFE/A DE LA OTI | RESPONSABLE

Anexo 02

Formato de informe técnico previo de evaluación

FORMATO INFORME TÉCNICO PREVIO DE EVALUACIÓN	
1. NOMBRE DEL ÁREA	
2. RESPONSABLE DE LA EVALUACIÓN	
3. CARGO	
4. FECHA	

- El presente informe se ha elaborado sobre la base del Decreto Supremo N° 024-2006-PCM Reglamento de la Ley N° 28612 - Ley que norma el uso, adquisición y adecuación del software en la Administración Pública.
- Las herramientas que se toman en consideración en el presente informe, son las disponibles en el mercado peruano, que cuenten con soporte local a través de una red de asociados de negocio que aseguren el adecuado soporte en el tiempo y la pluralidad de ofertas.
- Se ha tomado como referencia informes técnicos previos de software de otras entidades del Estado Peruano.

5. JUSTIFICACIÓN

Descripción de la necesidad que se pretende satisfacer y que deriva de los requerimientos formulados por las áreas usuarias.

6. ALTERNATIVAS

Dentro de las alternativas identificadas en el mercado local que ofrecen software de estas características tenemos:

Producto	Proveedor o Fabricante
01.	
02.	
03.	

Para la determinación de estas herramientas, así como para la evaluación técnica, se ha tomado como referencia:

a) Presentaciones de los representantes de las empresas proveedoras de soluciones de software.
b) La información disponible en la página web de cada uno de los fabricantes.
c) Información disponible en Internet.
d) Evaluaciones similares en otras instituciones del Estado Peruano.

7. ANÁLISIS COMPARATIVO TÉCNICO

El análisis comparativo técnico está basado en la metodología establecida en la Guía Técnica sobre Evaluación de Software para la Administración Pública, aprobada por Resolución Ministerial N° 139-2004-PCM.

7.1. Propósito de la evaluación

Identificar características de calidad mínimas para el software requerido.

7.2. Tipo de producto

Descripción del tipo de producto requerido

7.3. Modelo de Calidad

Se aplica el modelo establecido en la Guía Técnica sobre Evaluación de Software para la Administración Pública (R.M. N° 139-2004-PCM).

7.4. Selección de métricas

La selección de métricas se obtuvo a partir de los atributos especificados en el Modelo de Calidad, tal como se detalla en Anexo 02_A *"Atributos para la evaluación de software"*. Es necesario mencionar que, para cuantificar el resultado, luego de evaluar las alternativas del componente de software identificadas se asignará un (01) punto a cada característica técnica que *"SI"* cumpla con el atributo definido.

Se debe tomar en cuenta el peso de cada Sub-Característica y su correspondiente Característica, tanto para el Modelo de Calidad Interna y Externa, como para el Modelo de Calidad de Uso. La suma de los puntajes máximos de los atributos de Calidad Interna y Externa, con los de la Calidad de Uso, siempre será 100. Asimismo, el siguiente cuadro define el puntaje y el criterio para adoptar o no, una determinada alternativa:

Rango de Puntaje	Descripción
[75- 100>	**Altamente Recomendable.** Cumple totalmente con los requerimientos y expectativas.
[50-74>	**Riesgoso** Cumple parcialmente con los requerimientos, pero no se garantiza su adaptación a las necesidades.
[0-49>	**No recomendable.** Software con características inadecuadas.

7.5. Comparativo Técnico/Funcional

Describir el resultado de la evaluación por cada alternativa, agrupada desde el punto de vista del modelo de calidad sugerido por la Secretaría de Gobierno Digital (ex - ONGEI) de la PCM.

El detalle de la evaluación por cada funcionalidad se describe en el Anexo 03_A.

8. ANÁLISIS COMPARATIVO COSTO-BENEFICIO

Alternativa	Proveedor/Fabricante	Costo Referencial por Licencia

9. CONCLUSIONES

10. FIRMAS

Responsables de la emisión del informe y Jefe/a de la Oficina de Tecnologías de la Información

Anexo 02_A
Atributos para la evaluación de software

1.1 TABLA RESUMEN DE PUNTAJES MÁXIMOS POR CARACTERÍSTICAS

CARACTERÍSTICA	PUNTAJE MÁXIMO
CALIDAD INTERNA Y EXTERNA	
Funcionalidad	
Usabilidad	
Eficiencia	
Capacidad de Mantenimiento	
Portabilidad	
CALIDAD DE USO	
Eficacia	
Productividad	
Satisfacción	
Seguridad	

1.2 TABLA DETALLADA DE PUNTAJES MÁXIMOS POR CARACTERÍSTICAS/SUB-CARACTERÍSTICAS

CALIDAD INTERNA Y EXTERNA PUNTAJE MAXIMO:		
Característica	**Sub Característica**	**Puntaje Máximo**
Funcionalidad La capacidad del producto de software para proveer las funciones que satisfacen las necesidades explícitas e implícitas cuando el software se utiliza bajo condiciones Específicas. **Puntaje máximo:**	**Adecuación** La capacidad del producto de software para proveer un adecuado conjunto de funciones para las tareas y objetivos especificados por el usuario. Ejemplos de adecuación son la composición orientada a tareas de funciones a partir de sub funciones que las constituyen, y las capacidades de las tablas.	
	Exactitud La capacidad del producto de software para proveer los resultados o efectos acordados con un grado necesario de precisión.	
	Conformidad de funcionalidad La capacidad del producto de software de adherirse a los estándares, convenciones o regulaciones legales y prescripciones similares referentes a la funcionalidad.	
	Madurez La capacidad del producto de software para evitar fallas como resultado de errores en el software.	
Usabilidad La capacidad del producto de software para mantener un nivel específico de funcionamiento cuando se está utilizando bajo condiciones especificadas. **Puntaje máximo:**	**Entendimiento** La capacidad del producto de software para permitir al usuario entender si el software es adecuado, y cómo puede ser utilizado para las tareas y las condiciones particulares de la aplicación.	
	Aprendizaje La capacidad del producto de software para permitir al usuario aprender su aplicación. Un aspecto importante a considerar aquí es la documentación del software.	
	Operatividad La capacidad del producto de software para permitir al usuario operarlo y controlarlo.	
	Atracción La capacidad del producto de software de ser atractivo al usuario.	
Eficiencia La capacidad del producto de software para proveer un desempeño adecuado, de acuerdo a la cantidad de recursos utilizados y bajo las condiciones planteadas. **Puntaje máximo:**	**Comportamiento de tiempos** La capacidad del producto de software para proveer tiempos adecuados de respuesta y procesamiento, y ratios de rendimiento cuando realiza su función bajo las condiciones establecidas.	

CALIDAD INTERNA Y EXTERNA PUNTAJE MAXIMO:		
Característica	**Sub Característica**	**Puntaje Máximo**
Capacidad de mantenimiento Capacidad del producto de software para ser modificado. Las modificaciones pueden incluir correcciones, mejoras o adaptación del software a cambios en el entorno, y especificaciones de requerimientos funcionales y software del sistema, y materiales (Ej: Papel de impresión o diskettes). **Puntaje máximo:**	**Cambia** La capacidad del software para permitir que una determinada modificación sea implementada.	
Portabilidad La capacidad del software para ser trasladado de un entorno a otro. El entorno puede incluir entornos organizacionales, de hardware o de software. **Puntaje máximo:**	**Adaptabilidad** La capacidad del producto de software para ser adaptado a diferentes entornos especificados sin aplicar acciones o medios diferentes de los previstos para el propósito del software considerado.	
	Facilidad de Instalación La capacidad del producto de software para ser instalado en un ambiente especificado.	
	Coexistencia La capacidad del producto de software para coexistir con otros productos de software independientes dentro de un mismo entorno, compartiendo recursos comunes.	
	Reemplazar La capacidad del producto de software para ser utilizado en lugar de otro producto de software, para el mismo propósito y en el mismo entorno.	

MODELO DE CALIDAD DE USO PUNTAJE MÁXIMO:	
Característica	**Puntaje Máximo**
Eficacia La capacidad del producto de software para permitir a los/as usuarios/as lograr las metas especificadas con exactitud e integridad, en un contexto especificado de uso.	
Productividad La capacidad del producto de software para permitir a los/as usuarios/as emplear cantidades apropiadas de recursos, en relación a la eficacia lograda en un contexto especificado de uso.	
Satisfacción La capacidad del producto de software para satisfacer a los/as usuarios/as en un contexto especificado de uso.	
Seguridad La capacidad del producto de software para lograr niveles aceptables de riesgo de daño a las personas, institución, software, propiedad (licencias, contratos de uso de software) o entorno, en un contexto especificado de uso.	

ANEXO 03:

EVALUACIÓN DETALLADA DE LAS HERRAMIENTAS DE SOFTWARE

MODELO DE CALIDAD	CARACTERÍSTICA	SUBCARACTERÍSTICA	Atributo	Alternativa 1	Alternativa 2	Alternativa 3
Calidad Interna y Externa	Funcionalidad	Adecuación				
Calidad Interna y Externa	Funcionalidad	Exactitud				
Calidad Interna y Externa	Funcionalidad	Conformidad de Funcionalidad				
Calidad Interna y Externa	Funcionalidad	Madurez				
		Sub Total Funcionalidad				
Calidad Interna y Externa	Usabilidad	Entendimiento				
Calidad Interna y Externa	Usabilidad	Aprendizaje				
Calidad Interna y Externa	Usabilidad	Operatividad				
Calidad Interna y Externa	Usabilidad	Operatividad				
Calidad Interna y Externa	Usabilidad	Operatividad				
Calidad Interna y Externa	Usabilidad	Operatividad				
Calidad Interna y Externa	Usabilidad	Operatividad				
Calidad Interna y Externa	Usabilidad	Operatividad				
Calidad Interna y Externa	Usabilidad	Operatividad				
Calidad Interna y Externa	Usabilidad	Operatividad				
Calidad Interna y Externa	Usabilidad	Operatividad				
Calidad Interna y Externa	Usabilidad	Atracción				
Calidad Interna y Externa	Usabilidad	Atracción				
		Sub Total Usabilidad				
Calidad Interna y Externa	Eficiencia	Comportamiento de Tiempos				
		Sub Total Eficiencia				
Calidad Interna y Externa	Capacidad de Mantenimiento	Cambiable				
		Sub Total Capacidad de Mantenimiento				
Calidad Interna y Externa	Portabilidad	Adaptabilidad				

MODELO DE CALIDAD	CARACTERÍSTICA	SUBCARACTERÍSTICA	Atributo	Alternativa 1	Alternativa 2	Alternativa 3
Calidad Interna y Externa	Portabilidad	Facilidad de Instalación				
Calidad Interna y Externa	Portabilidad	Coexistencia				
Calidad Interna y Externa	Portabilidad	Reemplazar				
		Sub Total Portabilidad				
Calidad Interna y Externa						
Calidad de Uso	Eficacia	Eficacia				
			Sub Total Eficacia			
Calidad de Uso	Productividad	Productividad				
			Sub Total Productividad			
Calidad de Uso	Satisfacción	Satisfacción				
Calidad de Uso	Satisfacción	Satisfacción				
Calidad de Uso	Satisfacción	Satisfacción				
Calidad de Uso	Satisfacción	Satisfacción				
Calidad de Uso	Satisfacción	Satisfacción				
Calidad de Uso	Satisfacción	Satisfacción				
			Sub Total Satisfacción			
Calidad de Uso	Seguridad	Seguridad				
			Sub Total Seguridad			
Calidad de Uso						
Puntaje Total						

Instructivo de gestión de incidentes de seguridad de información y ciberseguridad

I. OBJETIVO

Definir las acciones para gestionar los incidentes de seguridad de la información y ciberseguridad.

II. INSTRUCCIONES

1. Reportar la debilidad, evento o incidente: El/La usuario/a notifica la debilidad, evento o incidente a través del aplicativo de mesa de ayuda, o a el/la Oficial de Seguridad y Confianza Digital (en adelante, OSCD) a través de correo institucional oficial-seguridad@oefa.gob.pe, comunicación verbal, plataforma de mensajería o cualquier otro medio autorizado.

2. Registro de debilidad, evento o incidente: El/La Oficial de Seguridad y Confianza Digital registra los datos del PA0303-F02 *"Registro de incidentes SI y Ciberseguridad"* en la Sección I - Identificación de la notificación, consignando la siguiente información:
   - N° de Ticket
   - Medio de la notificación (verbal, correo institucional, telefónico, etc.)
   - Fecha y hora de la detección
   - Fecha y hora de la notificación

   Se debe identificar a el/la usuario/a que notifica, llenando los campos de la Sección II del formato PA0303-F02 Registro de incidentes de SI y Ciberseguridad.

3. Determinar la naturaleza de la debilidad, evento o incidente: El OSCD debe evaluar la notificación del usuario y determinar si se trata de una debilidad, evento o incidente aplicando el siguiente criterio:

   - Si lo notificado no es un hecho y se evidencia la ineficacia de un control o la falta de control de seguridad de la información que podría exponer la confidencialidad, integridad o disponibilidad de un activo de información o infraestructura tecnológica, se clasificará como una debilidad. Se asignará un número de debilidad en la sección IV del formato de Registro de Incidentes y se pueden realizar análisis de vulnerabilidades tecnológicas y pruebas de intrusión.

   - Si lo notificado es un hecho, se clasificará como un evento y se determinará su magnitud utilizando la Tabla 1 *"Clasificación de la notificación del usuario"* en la sección V del Registro de Incidente.

4. Registrar incidentes: El OSCD evalúa si el evento es un incidente de seguridad de la información empleando el Registro de Incidentes - Sección V, para lo cual se podrá solicitar apoyo a otras Unidades de OEFA, incluyendo el Comité de Líderes.

   El OSCD para efectuar la evaluación debe poner énfasis en el activo, activos de información y/o plataforma tecnológica afectados (sección 4.3 del formato PA0303-F02 Registro de incidentes SI y Ciberseguridad), así como en el control o controles

de seguridad de la información que fallaron y ocasionaron el evento (sección 4.4 del formato PA0303-F02 Registro de incidentes SI y Ciberseguridad).

Finalmente, deberá designar un Gestor del Incidente de Seguridad de la Información quien se encargará de la siguiente actividad.

5. El Gestor de incidente de seguridad de la información debe coordinar las respuestas, de contención y erradicación, al evento/incidente de seguridad de la información conteniendo los efectos negativos del evento. El Gestor puede recurrir a todas las instancias posibles para responder al evento/incidente. Las respuestas deben ser registradas en el Registro de Incidentes – Secciones VI y VII.
   Nota: El Gestor debe evaluar si el incidente está evolucionando de tal forma que se puede constituir en un desastre y activar el PCO.

6. Validar respuestas: El OSCD debe validar si las respuestas al evento/incidente de seguridad de la información ha contenido de manera efectiva los efectos negativos del evento, y si se ha erradicado el mismo. La validación debe ser registrada en el Registro de Incidentes- Sección 7.7. Si las respuestas no son eficaces se debe notificar al Gestor y continuarse en el con la actividad 5, sino continuar con las actividades. Se deberá signar un estado para el seguimiento/control del evento o incidente
   Nota:
   el OSCD debe evaluar si el incidente está evolucionando de tal forma que se puede constituir en un desastre y activar el PCO.

7. Analizar causa del evento/incidente: El OSCD debe analizar la causa del evento/incidente de seguridad de la información empleando la técnica de los 5 por qué u otra similar. El análisis de causa y la identificación de la causa debe ser registrada en el Registro de Incidentes- Sección X.

8. El OSCD debe evaluar si la causa del evento de seguridad de la información amerita una acción correctiva que impida la ocurrencia del evento/incidente en el futuro. La decisión debe ser registrada en el Registro de Incidentes- Sección XII

9. Cierre del evento/incidente: El OSCD debe dar por cerrado el evento cuando se trató de uno como tal y no de un incidente, si se trató de un incidente se debe continuar con las actividades siguientes.

10. El OSCD debe iniciar una acción correctiva a la causa del incidente de seguridad de la información a fin de evitar la ocurrencia del incidente en el futuro. Se debe registrar el inicio de la acción correctiva empleando el Registro de Acciones correctivas sección XII.

    El OSCD debe evaluar si el evento de seguridad de la información amerita llevar a cabo una oportunidad de mejora, en caso se lleva a cabo se debe emplear el Registro de Oportunidades de mejora. La decisión debe ser registrada en el Registro de Incidentes- Sección 12.2.

FORMATO DE REGISTRO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

I. Identificación de la notificación

1.1 Nro. Notificación		1.3 Fecha de la detección		1.5 Hora Detección	
1.2 Medio de la notificación	Teléfono	1.4 Fecha de la notificación		1.6 Hora notificación	

II. Identificación del notificante

2.1 Nombre y apellido		2.5 Email	
2.2 Cargo		2.6 Teléfono	
2.3 Unidad			

III. Sobre la notificación (Posible debilidad, evento o incidente de seguridad de la información)

3.1 ¿Es un hecho?	
3.2 Descripción	

IV. Clasificación de la debilidad, evento o incidente de seguridad de la información

4.1 ¿Es debilidad?		4.2 Nro. Debilidad	

	4.3.a.- Nombre del activo de información	4.3.b.- Ámbito	4.3.c.- Ubicación del activo
4.3 Activos de información afectado o comprometidos			

	4.4.a.- Descripcion del Control
4.4 Controles que resultan ineficaces (o no existentes)	

V. Categorización del evento de seguridad de la información

5.1 Magnitud		5.2 Duración	
		5.3 CLASIFICACIÓN	

VI. Gestión del evento o incidente de seguridad de la información

6.1 Nombre del gestor		6.2 Fecha estimada de cierre	
6.3 Nro. Incidente			

VII. Respuestas de Contención

7.1 Nro.	7.2 Responsable	7.3 Descripción	7.4 Fec. Inicio	7.5 Fecha Fin	7.6 Estado

7.7 Eficacia	

VIII. Respuestas de erradicación

8.1 Nro.	8.2 Responsable	8.3 Descripción	8.4 Fec. Inicio	8.5 Fecha Fin	8.6 Estado

8.7 Eficacia	

IX. Seguimiento y control

9.1 Estado		9.2 Fecha estado	

X. Análisis de causa

10.1 Análisis de causa	
10.2. Descripción de la causa raiz	

XI. Lecciones aprendidas

11.1 Descripción	

XII. Evaluación de acciones a tomar

12.1 ¿Tomar acción correctiva?		12.2 ¿Tomar oportunidad de mejora?	

XIII. Comunicación al Usuario que notificó

13.1 ¿Se notificó al usuario?		13.2 Medio empleado	
13.3 ¿Se notificó efectivamente?		13.4 Fecha de la notificación	
13.5 Comentarios / Observaciones			