Oefa Organismo de Evaluación y Fiscalización Ambiental	**FICHA DE PROCEDIMIENTO**	Código: PA0304 Versión: ***03*** Fecha: 22/12/2022

NOMBRE DEL PROCEDIMIENTO	Monitoreo y mantenimiento de la infraestructura de tecnologías de la información

APROBACIÓN		
Nombre y cargo	**Órgano o Unidad Orgánica**	**Firma y sello**
Elaborado por: Zico Alexis Yacila Espinoza 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: YACILA ESPINOZA Zico Alexis FAU 20521286769 soft Cargo: Jefe de la Oficina de Tecnologías de la Información Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento
Revisado por: Elvis Romel Palomino Pérez Jefe de la Oficina de Planeamiento y Presupuesto	Oficina de Planeamiento y Presupuesto	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: PALOMINO PEREZ Elvis Romel FAU 20521286769 soft Cargo: Jefe de la Oficina de Planeamiento y Presupuesto Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento
Revisado por: Gonzalo Pinto Bazurco Mendoza Jefe de la Oficina de Asesoría Jurídica	Oficina de Asesoría Jurídica	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: PINTO BAZURCO MENDOZA Gonzalo FAU 20521286769 soft Cargo: Jefe de la Oficina de Asesoría Jurídica Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento
Aprobado por: Miriam Alegría Zevallos Gerenta General	Gerencia General	Oefa Organismo de Evaluación y Fiscalización Ambiental Firmado digitalmente por: ALEGRIA ZEVALLOS Miriam FAU 20521286769 soft Cargo: Gerenta General Lugar: Sede Central - Lima\Lima\Jesus Maria Motivo: Soy el autor del documento

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: PA0304 Versión: ***03*** Fecha: 22/12/2022

CONTROL DE CAMBIOS		
Versión	**Sección del Procedimiento**	**Descripción del cambio**
01	Todas las secciones	- Se actualiza el alcance. - Se incorporan normas a la base normativa. - Se modifican las consideraciones generales. - Se incorporan definiciones. - Se actualizan las actividades.[2]
02	Base Normativa Anexo del procedimiento	- Se incorporan norma a la base normativa. - Se actualiza el Instructivo I-OTI-PA0304-1 *"Mantenimiento de Base de datos"*, el Instructivo I-OTI-PA0304-2 *"Operaciones de Tecnologías de la Información"*. - Se adecúa el versionamiento de los formatos a la versión del procedimiento[3]
03	***Definiciones, actividades y anexos del procedimiento***	- ***Se procedió a realizar precisiones en la base normativa, definiciones, actividad N° 1 y 4. Asimismo, se incluyó nuevas actividades N° 9, 10, 11 y 12 relacionadas a la gestión de cambios.*** - ***Se precisan formatos como la Solicitud de acceso privilegiado y el Registro de altas, bajas, modificaciones de usuarios con acceso privilegiado.*** - ***Se modifican los instructivos I-OTI-PA0304-1 "Mantenimiento de Base de datos", I-OTI-PA0304-2 "Operaciones de TI", se cambia la denominación del instructivo I-OTI-PA0304-3 "Mantenimiento de redes y telecomunicaciones" por "Mantenimiento de redes y comunicaciones"[4].***

OBJETIVO	Establecer las actividades para administrar y ejecutar el monitoreo y mantenimiento de la infraestructura de Tecnologías de la Información (TI) que permita que los servicios de TI se brinden de manera confiable y consistente.
ALCANCE	El presente procedimiento es de aplicación obligatoria de la Oficina de Tecnologías de la Información. Comprende desde el registro de la solicitud o alerta hasta su cierre en el aplicativo de mesa de ayuda.
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 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. - Decreto Supremo N° 013-2017-MINAM, Decreto Supremo 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. - ***Decreto Supremo N° 103-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.*** - Resolución Ministerial N° 073-2004-PCM, que aprueba la Guía para la Administración Eficiente del Software Legal en la Administración Pública.

[2] Modificado mediante Resolución de Gerencia General N° 051-2021-OEFA/GEG del 9 de junio de 2021.

[3] Modificado mediante Resolución de Gerencia General N° 0063-2022-OEFA/GEG del 26 de mayo de 2022.

4 Modificado mediante Resolución de Gerencia General N° 00114-2022-OEFA/GEG del 22 de diciembre de 2022.

	- 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. 3a 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 del 04 de mayo del 2022 que aprueba la designación y funciones del Oficial de Seguridad y Confianza Digital del OEFA. - Resolución de Gerencia General N° 051-2020-OEFA/GEG, que aprueba las *"Políticas Específicas de Seguridad de la Información del Organismo de Evaluación y Fiscalización Ambiental - OEFA"*, vinculadas a la implementación 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"*, aprobada por la Resolución Ministerial N° 004-2016-PCM, modificada por las Resoluciones Ministeriales números 166-2017-PCM y 087-2019-PCM. Las referidas normas incluyen sus modificatorias.
CONSIDERACIONES GENERALES	Las operaciones de Tecnologías de la Información están relacionadas a todo el proceso de mantenimiento de la infraestructura requerida para que las operaciones de TI no pierdan continuidad y se genere un respaldo de todas las acciones e información generada en el desarrollo de los procesos de TI.
DEFINICIONES	- **Alerta:** Notificaciones emitidas de la herramienta de monitoreo en referencia a la ocurrencia de eventos en la infraestructura o un sistema informático. - **Aplicativo de mesa de ayuda:** Aplicativo informático que permite el registro y seguimiento de las solicitudes de servicios de TI. - **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. - **Componente:** Relacionados a servicios de base de datos, servidores, redes y telecomunicaciones. - ***Gestión de cambio: Práctica de TI diseñada para minimizar las interrupciones en los servicios de TI mientras se realizan cambios en sistemas o en los servicios. Un cambio es agregar, modificar o eliminar cualquier cosa que pueda repercutir directa o indirectamente en los servicios.*** - **Herramienta de monitoreo:** Herramientas que permiten recolectar, analizar y utilizar información para hacer seguimiento al desempeño de las redes, servidores y aplicaciones. - **Infraestructura:** Conjunto de dispositivos físicos y aplicaciones de software que se requieren para operar toda la Entidad. - **Reporte de mantenimiento:** Documento que detalla las actividades realizadas para la atención de una solicitud o alerta. - **Ticket:** Consulta de cualquier tipo que realiza el área usuaria o la Oficina de Tecnologías de la Información.
SIGLAS	- 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 o alerta	Áreas usuarias

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
1	Recibir, verificar y registrar la solicitud de servicio de TI o la alerta	Recibe la solicitud de atención de servicios de TI ***mediante ticket generado por la aplicación de mesa de ayuda o la alerta, a través de correo institucional.*** Verifica si la atención corresponde a una solicitud de servicio de TI o a una alerta emitida por la herramienta de monitoreo y la registra en el aplicativo de mesa de ayuda. **¿A qué tipo de atención corresponde?** - **Solicitud de servicio de TI:** Va la actividad N° 2. - **Alerta:** Va a la actividad N° 4. Cambia el estado de la solicitud de servicio de TI o alerta a "*en espera"*.	***Correo institucional*** ***Ticket***	Operador/a de soporte técnico	OTI
2	Verificar el catálogo de servicios de TI	Verifica que el servicio solicitado se encuentre en el catálogo de servicios de TI. **¿Servicio se encuentra en catálogo de servicio?** **Sí:** Va a la actividad N° 4. **No:** Va a la actividad N° 3. **Plazo:** En el día hábil de registrada la solicitud.	-	Operador/a de soporte técnico	OTI
3	Registrar un nuevo servicio de TI en el catálogo de servicios	Registra un nuevo servicio en el catálogo de servicios de TI. Va a la actividad N° 2. **Plazo:** Tres (3) días hábiles luego del ingreso de un nuevo servicio.	Catálogo de servicios de TI	Operador de soporte técnico	OTI
4	Identificar el tipo de componente para asignar a el/la Analista correspondiente	Identifica el componente (base de datos, servidores o redes y ***comunicaciones***) para asignar directamente a el/la Analista de Infraestructura correspondiente. **¿Cuál es el tipo de componente?** - **Base de datos:** Va a la actividad N° 5. - **Servidores:** Va a la actividad N° 6. - **Redes y *comunicaciones*:** Va a la actividad N° 7. Cambia el estado de la solicitud de servicio de TI o alerta a "*asignado en curso*".	Aplicativo de Mesa de Ayuda	Operador de soporte técnico	OTI

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
5	Atender y dar mantenimiento de base de datos	Atiende la solicitud de servicio de TI o alerta de monitoreo; y realiza el mantenimiento de acuerdo con el Instructivo *I-OTI-PA0304-1 "Mantenimiento de Base de datos"*. **¿Cuál es el tipo de atención?** - **Alerta:** Va a la actividad N° 8. - ***Gestión de cambio: Va a la actividad N° 9*** - **Solicitud:** Va a la actividad N° ***13.*** Cambia el estado de la solicitud de servicio de TI a "*resuelto*".	Aplicativo de Mesa de Ayuda	Analista de administración de base de datos	OTI
6	Atender y dar mantenimiento de servidores	Atiende la solicitud de servicio de TI o alerta de monitoreo; y, realiza el mantenimiento de acuerdo con el instructivo *I-OTI-PA0304-2 "Operaciones de Tecnologías de la Información"*. **¿Cuál es el tipo de atención?** - **Alerta:** Va a la actividad N° 8. - ***Gestión de cambio: Va a la actividad N° 9*** - **Solicitud:** Va a la actividad N° ***13.*** Cambia el estado de la solicitud de servicio de TI a "*resuelto*".	Aplicativo de Mesa de Ayuda	Analista de redes	OTI
7	Atender y dar mantenimiento de redes y comunicaciones	Atiende la solicitud de servicio de TI o alerta de monitoreo; y realiza el mantenimiento de acuerdo con el Instructivo I-OTI-PA0304-3 *"Mantenimiento de redes y **comunicaciones**"*. **¿Cuál es el tipo de atención?** - **Alerta**: Va a la actividad N° 8. - ***Gestión de cambio: Va a la actividad N° 9*** - **Solicitud:** Va a la actividad N° ***13.*** Cambia el estado de la solicitud de servicio de TI a "*resuelto*".	Aplicativo de Mesa de Ayuda	Analista de redes y comunicaciones	OTI
8	Elaborar el reporte de mantenimiento	Elabora el reporte de mantenimiento y luego de atendida la solicitud o alerta comunica, mediante correo institucional, al equipo de infraestructura las actividades realizadas, así como a los/as usuarios/as de corresponder.	Reporte de mantenimiento Correo institucional	Analista de redes	OTI

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
9	***Dar conformidad al cronograma de actividades***	***El/la Analista de administración de base de datos o Analista de redes o Analista de redes y comunicaciones elaboran un cronograma detallando las actividades de Gestión de cambio, responsables, fechas e impacto (a nivel de proceso y seguridad de la Información) y lo remiten, mediante correo institucional, a el/la Gestor/a de Infraestructura y comunicaciones.*** ***El/La Gestor/a de Infraestructura y comunicaciones revisa y da la conformidad al Cronograma de actividades, comunicando su decisión a los/las Analistas, mediante correo institucional.*** ***Nota:*** ***En caso de que el/la Gestor/a de Infraestructura y comunicaciones encuentre observaciones al Cronograma de actividades, las comunica a los/las analistas para su subsanación y posterior revisión y conformidad.***	***Cronograma de actividades***	***Analista de administración de base de datos*** ***Analista de redes*** ***Analista de redes y comunicaciones*** ***Gestor/a de Infraestructura y comunicaciones***	***OTI***
10	***Aprobar el cambio de configuración o componentes***	***El/la Gestor de infraestructura y comunicaciones convoca a una reunión a Gestor/a de calidad, Coordinador/a de soluciones de Tecnológicas, Supervisor de Proyectos de Desarrollo de Sistemas y a el/la Jefe/a de la OTI para informar el cambio propuesto más el cronograma de actividades y la respectiva aprobación de los mismos por parte de el/la Jefe de la OTI.*** ***¿El/La Jefe/a de la OTI aprueba el cambio y el cronograma de actividades?*** ***Si: Va a la actividad N° 11*** ***No: Indica los ajustes respectivos. Va a la actividad N° 9*** ***Nota 1:*** ***El/La Analista de administración de base de***	***Acta de Reunión*** ***Correo institucional***	***Jefe/a de la OTI*** ***Gestor/a de Infraestructura y comunicaciones Analista de administración de base de datos*** ***Analista de redes*** ***Analista de redes y comunicaciones*** ***Gestor/a de calidad*** ***Coordinador/a de soluciones de Tecnológicas*** ***Supervisor de Proyectos de Desarrollo de Sistemas***	***OTI***

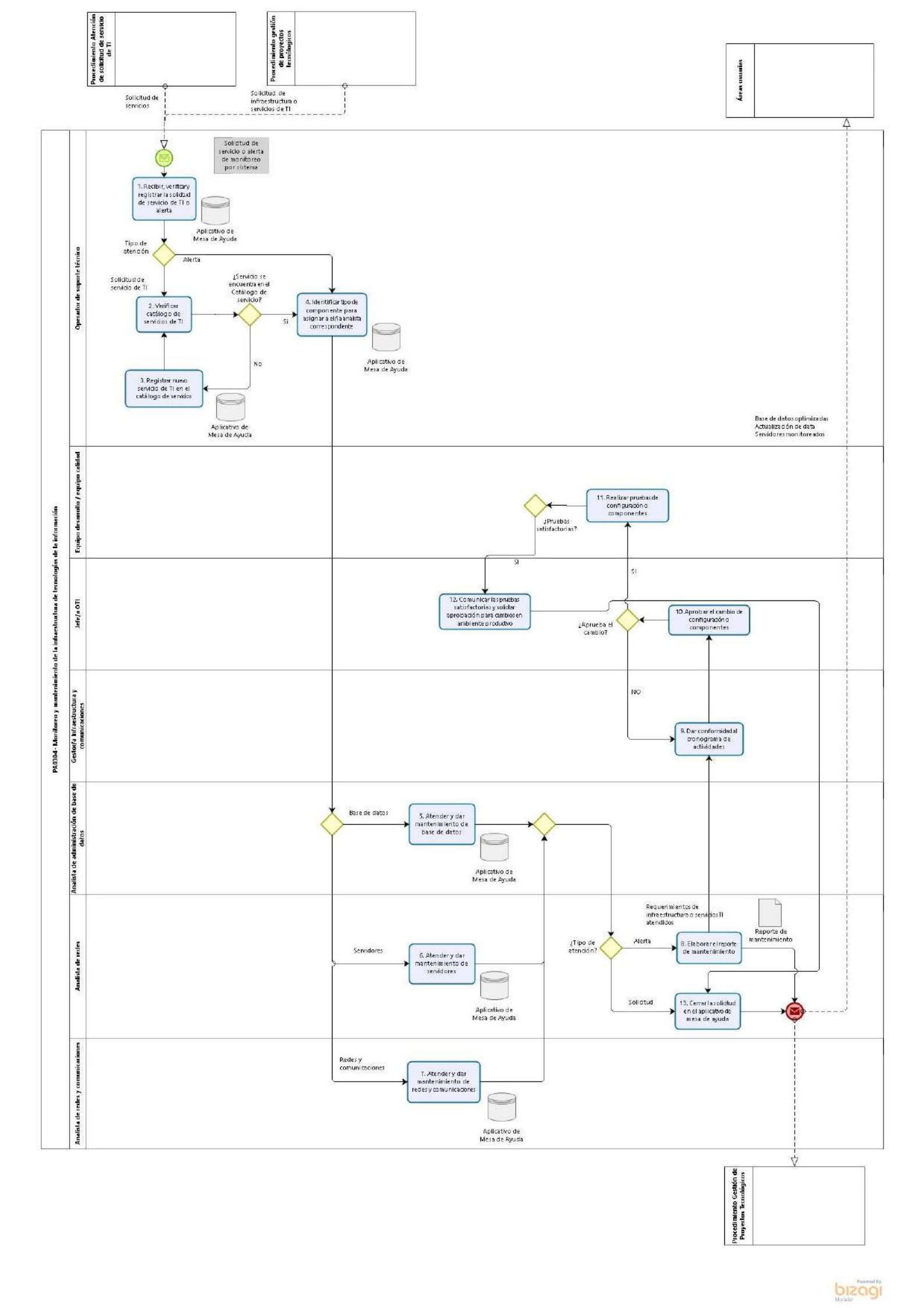
ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
		datos, Analista de redes y/o analista de redes y comunicaciones acompañan en la reunión al gestor de infraestructura y comunicaciones. ***Nota 2:*** ***Luego de ser aprobado el cambio el/la Analista de administración de base de datos o Analista de redes o Analista de redes y comunicaciones genera el ticket de Gestión de cambio en el Aplicativo de Mesa de Ayuda.*** ***Nota 3: Culminada la reunión el Gestor/a de Infraestructura y comunicaciones elabora el Acta de Reunión con los acuerdos tomados; en caso no se lleve la reunión, se informará y aprobará mediante correo institucional.***			
11	***Realizar pruebas de configuración o componentes***	***El/La Analista de administración de base de datos o Analista de redes o Analista de redes y comunicaciones realiza las pruebas respectivas de acuerdo a:*** ***a. Cambios de base de datos: comunicar a equipo de desarrollo y calidad para las pruebas respectivas (de corresponder)*** ***b. Cambios de infraestructura: comunicar a equipo de desarrollo y calidad para las pruebas respectivas (de corresponder*** ***¿Las pruebas son satisfactorias?*** ***Si: va a la actividad N° 12*** ***No: revisa y dan solución a las observaciones. Va a la actividad N° 12***	***Pruebas***	***Analista programador*** ***Analista de calidad*** ***Analista de administración de base de datos*** ***Analista de redes*** ***Analista de redes y comunicaciones***	***OTI***

ACTIVIDADES				**EJECUTOR**	
N°	**ACTIVIDAD**	**DESCRIPCIÓN**	**REGISTROS**	**RESPONSABLE**	**UNIDAD DE ORGANIZACIÓN**
12	***Comunicar las pruebas satisfactorias y solicitar aprobación para cambios en ambiente productivo***	***El/la Gestor de infraestructura y comunicaciones y/o el/la analista de infraestructura comunica al Jefe de la OTI que las pruebas son satisfactorias y solicita aprobación para cambios en ambiente productivo.*** ***El/La Jefe/a de la OTI comunica a Gerencia General los cambios y con la aprobación se remite un correo institucional a todos los/las usuarios/as de la Entidad indicando la indisponibilidad de los servicios que se verán afectados para la puesta en producción de los nuevos cambios.***	***Correo institucional***	***Jefe/a*** ***Gestor de infraestructura y comunicaciones*** ***Analista de infraestructura***	***OTI***
13	***Cerrar la solicitud en el aplicativo de mesa de ayuda***	***Cierra el ticket de atención de la solicitud o alerta y registra el detalle de la solución realizada en el aplicativo de mesa de ayuda.*** ***Fin del procedimiento.***	***Aplicativo de Mesa de Ayuda***	***Analista de redes***	***OTI***

DOCUMENTOS QUE SE GENERAN:
Catálogo de servicios Reporte de mantenimiento Ticket de atención

ANEXO DEL PROCEDIMIENTO:
- Instructivo I-OTI-PA0304-1: *"Mantenimiento de Base de datos".* - Instructivo I-OTI-PA0304-2: *"Operaciones de Tecnologías de la Información".* - Instructivo I-OTI-PA0304-3: *"Mantenimiento de redes y* ***comunicaciones****".* - ***Solicitud de acceso privilegiado*** - ***Registro de altas, bajas ,modificaciones de usuarios con acceso privilegiado***

PROCESO RELACIONADO
PA03 - Tecnologías de la información


Procedimiento Atención de solicitud de servicio de TI
Procedimiento gestión de proyectos tecnológicos
Áreas usuarias
Solicitud de servicios
Solicitud de infraestructura o servicios de TI
P8.03.04- Monitoreo y mantenimiento de la infraestructura de tecnologías de la información
Operador de soporte técnico
Equipo desarrollo / equipo calidad
Jefe/a OTI
Gestor/a Infraestructura y comunicaciones
Analista de administración de base de datos
Analista de redes
Analista de redes y comunicaciones
Solicitud de servicio o alerta de monitoreo por sistema
1. Recibir, verificar y registrar la solicitud de servicio de TI o alerta
Aplicativo de Mesa de Ayuda
Tipo de atención
Alerta
Solicitud de servicio de TI
2. Verificar catálogo de servicios de TI
¿Servicio se encuentra en el Catálogo de servicio?
Si
No
3. Registrar nuevo servicio de TI en el catálogo de servicios
4. Identificar tipo de componente para asignar a el/la analista correspondiente
Base de datos optimizadas
Actualización de data
Servidores monitoreados
11. Realizar pruebas de configuración o componentes
¿Pruebas satisfactorias?
12. Comunicar las pruebas satisfactorias y solicitar aprobación para cambios en ambiente productivo
¿Aprueba el cambio?
10. Aprobar el cambio de configuración o componentes
9. Dar conformidad al cronograma de actividades
Base de datos
5. Atender y dar mantenimiento de base de datos
Servidores
6. Atender y dar mantenimiento de servidores
Redes y comunicaciones
7. Atender y dar mantenimiento de redes y comunicaciones
Requerimientos de infraestructura o servicios TI atendidos
¿Tipo de atención?
Alerta
Solicitud
8. Elaborar el reporte de mantenimiento
Reporte de mantenimiento
13. Cerrar la solicitud en el aplicativo de mesa de ayuda
Procedimiento Gestión de Proyectos Tecnológicos

Instructivo de mantenimiento de base de datos

I. OBJETIVO

Establecer las tareas para facilitar el correcto funcionamiento de las operaciones de tecnologías de la información a nivel de base de datos considerando los tickets de atención de solicitudes (en adelante, ***ticket***) y el monitoreo de la infraestructura.

II. INSTRUCCIONES

Para la administración de base datos, se observa lo siguiente:

2.1. Creación de base de datos

2.1.1 En relación a la creación de usuarios/as en las bases de datos, se deben seguir las siguientes acciones:

a) Se inicia la atención a través de un ticket o correo institucional, con la solicitud de atención para la creación de usuarios.

b) El/La Administrador/a de Base de Datos (en adelante, ***el ABD***) procede a revisar el tipo de usuario/a que se creará, siguiendo los siguientes criterios:

i. En caso se trate de un/a usuario/a de las áreas del OEFA se crea el usuario y se asigna los privilegios de consulta, registrándose en la bitácora de credenciales, previamente con la aprobación de el/la Jefe/a de la Oficina de Tecnologías de la Información. Posterior a ello, comunica, mediante correo institucional a los/las usuarios/as y finaliza la atención.
En esta atención se incluyen a aquellos/as usuarios/as que solicitan acceso y privilegios donde se encuentran la información de los bancos de datos personales de la Entidad para su tratamiento.

ii. En caso que sea un/a usuario/a creado por la Oficina de Tecnologías de la Información (en adelante, ***la OTI***), para los diversos aplicativos o sistemas de información se ingresa al terminal de línea de comando de el/la analista de Base de Datos y procede a crear el usuario, para ello se debe definir la base de datos donde se creará el usuario y asignarle una contraseña. Para esta actividad se consideran la creación de tres (03) tipos de usuarios:

- **<u>Usuario esquema</u>**:

  Para crear un usuario de esquema, se procede a:
  - Calcular la tasa de crecimiento de la base de datos (***ver Anexo N° 1).***
  - Se asigna el espacio requerido y los privilegios de usuario esquema.
  - Se revisa el *Estándar de base de datos y se* procede a registrar en la bitácora de credenciales.
  - Si las credenciales no pertenecen a producción se procede a remitir las credenciales y cadena de conexión al usuario, de lo contrario se finaliza la atención.

- **<u>Usuario aplicación:</u>**
  Para crear un usuario de aplicación se procede a:
  - Asignar privilegios.

- Se registra en la bitácora de credenciales.
- ***Se remiten las credenciales y la cadena de conexión al usuario/a solicitante.***
- Si las credenciales no pertenecen al ambiente de producción se procede a remitir las credenciales y la cadena de conexión al usuario, de lo contrario se finaliza la atención.

➢ **<u>Usuario DBlink[1]</u>**
Para crear un usuario de DBlink se procede a:
- Asignar los privilegios de intercomunicación de base de datos
- Se procede a cerrar la atención del requerimiento.

2.1.2 En relación a la configuración de base de datos se deben realizar las siguientes acciones:

a) La configuración de base de datos inicia después de la creación de la misma, modificando los parámetros de configuración.
b) Se define el tamaño del FRA (Flash Recovery), estableciendo un valor inicial de 200 GB.
c) Se define el tamaño de Redo log[2], el cual se deja con su valor por defecto de 50 MB.
d) Se determina el número de grupos, cuatro (04) para DB Rac[3] y tres (03) para standlone[4], se define la multiplexación.
e) Se monitorea el espacio lógico (almacenamiento) y el tamaño del SGA[5] para poder comprobar que los valores establecidos son los indicados o si es necesario realizar una modificación como parte de un mantenimiento debido al crecimiento de la base de datos, para ello se siguen los siguientes criterios:

➢ *En relación al espacio físico*
- Se monitorea cada mes el crecimiento de la base de datos.
- Se calcula la tasa de crecimiento y con los datos obtenidos se procede a decidir si se requiere modificar el espacio.
- En caso no se decide modificar el espacio, se continúa con el monitoreo mensual y se actualizan los datos correspondientes al crecimiento de la base de datos.
- En caso se decida modificar el espacio, redefine el espacio con los datos obtenidos del monitoreo de crecimiento de la base de datos. Luego de establecer el nuevo tamaño se sigue con el monitoreo mensual.

➢ *Respecto al tamaño de SGA*

---

1 Es un tipo de objeto que permite realizar una conexión desde una base de datos a otra.

2 Redo log: los registros de rehacer comprenden archivos en un formato propietario que registra un historial de todos los cambios realizados en la base de datos.

3 DB Rac: es una característica incluida en el software de Oracle que permite la creación de clusters de base de datos (llamado Real Application Cluster - RAC).

4 Una base de datos standalone, quiere decir que está configurada para ser usada en una sola máquina no tiene alta disponibilidad.

5 SGA Área Global del Sistema) es una estructura básica de memoria de Oracle que sirve para facilitar la transferencia de información entre usuarios y también almacena la información estructural de la base de datos más frecuentemente requerida.

- Se procede a monitorear el SGA, de acuerdo a lo especificado en el literal b) del subnumeral 2.3.1 del acápite II.3 del presente instructivo.
- Según los datos obtenidos se redefine el tamaño y se continúa monitoreando el SGA

2.2. Atención de solicitudes de base de datos

a) Se inicia con un ticket o correo institucional, solicitando la atención de un requerimiento de base de datos.
b) Se verifica el tipo de script a ejecutar, pudiendo ser: *(i)* script de tipo DML (Data Manipulation Language); o, *(ii)* script de tipo DDL (Data Definition Language).

Si se trata de un script de tipo DML, se desarrollan las siguientes acciones:

- Se verifican los datos del correo, los cuales son la petición a realizar, la base de datos, el esquema y la ruta donde se encuentran los scripts a ejecutar.
- Se ingresa a la ruta donde se encuentran los scripts.
- Se verifica si el sustento de la petición se encuentra junto con los scripts, en caso de no contar con el sustento, se solicita que el usuario guarde el sustento dentro de la ruta de los scripts para poder continuar con la ejecución de la solicitud.
- Después de verificar que el sustento se encuentre en la ruta junto a los scripts, se realiza el backup de los objetos que serán afectados.
- Se ejecuta el script.
- Se validan los resultados, comprobando que el resultado sea igual al descrito en la solicitud.
- En caso el resultado no coincida se realiza un roollback y se informa, mediante correo institucional, a el/la usuario, quedando a la espera de su respuesta para continuar con la atención de la solicitud.
- Cuando el resultado coincide se ejecuta el commit y se procede a informar al usuario y cerrar la solicitud.

Si se trata de un script de tipo DDL, se desarrollan las siguientes *acciones*:

- Se verifica si se encuentran todos los requisitos, de no cumplir con los requisitos se procede a rechazar la solicitud y se informa, mediante correo institucional a el/la usuario/a.
- Se realiza el despliegue en ambiente de producción, siguiendo los pasos de desplegar aplicaciones, conforme al instructivo I-OTI-PA0304-2 "*Operaciones de Tecnologías de la Información"* (despliegue a producción de base de datos), procediendo a cerrar la solicitud.

Si se trata de acceso a una tabla de producción:
- ***Se realiza la solicitud mediante el Anexo N° 2 de solicitud de acceso a la base de datos.***
- ***Se remite previamente autorizado por el/la Jefe/a de Tecnologías de la Información.***
- ***Dicho acceso sólo es de lectura a la base de datos y se brinda solo a personal desarrollador de tecnologías de la información.***

2.3. Monitorear base de datos

a) En relación a la actualización (upgrade) de la versión de la base de datos, se desarrollan las siguientes acciones:
   - En coordinación con el equipo de desarrollo, se realiza un listado de las aplicaciones que se tiene en el ambiente productivo.

- El/La Analista de Administración de base de datos elabora un cronograma con las aplicaciones a probar en los ambientes de desarrollo, calidad. Si en estos ambientes no se presenta ningún inconveniente por la nueva versión de la base de datos, entonces se coordina con el/la Jefe/a de la OTI para realizar la actualización en el ambiente productivo (previa coordinación con GEG).

b) En relación al monitoreo de DB Time, el/la Analista de Administración de base de datos desarrolla las siguientes acciones:

- Inicia llevando un registro del DB Time (cuánto trabaja una Base de Datos por día).
- Se establece una medida base con los datos registrados.
- Se empieza a monitorear el DB Time con la medida base establecida.
- Se verifica que el valor del monitoreo se encuentre en el rango establecido por la medida base.
- Si se mantiene dentro del rango, no se ejecutará ninguna acción, pero se continuará monitoreando.
- En caso el valor se encuentre fuera del rango, se empiezan a buscar las causas, las cuales pueden ser:

  - Sentencias SQL: en caso el problema se encuentre en las sentencias SQL, se realiza el diagnóstico con el gestor de BD, se evalúa el reporte del diagnóstico, el cual determinará si se tiene que contactar con un desarrollador o realizar mejoras que se recomiendan en el diagnóstico. Después de realizar las mejoras en las sentencias, se seguirá con el monitorio para observar el resultado de las mejoras.
  - Tamaño incorrecto de SGA: en este caso se calcula el nuevo tamaño que debe tener el SGA, luego se verifica si se cuenta con espacio físico, en caso de no contar con espacio se solicita al personal correspondiente el aumento de la memoria RAM del servidor donde se encuentra la base de datos, ejecutando el aumento en base a la configuración de servidores informáticos.
  - Luego de confirmar que se tiene espacio para ampliar el SGA, se programa un mantenimiento de SGA, se apaga la base de datos y se ejecuta el mantenimiento planificado, luego se inicia la base de datos, se verifica que se inició correctamente y se monitorea el DB Time para ver reflejado la mejoras.

c) En relación a la expiración de las contraseñas de usuario de base de datos
Cada tipo de usuario de base de datos tiene un perfil asociado el cual se encuentra registrado en la herramienta de base de datos, esta herramienta de manera automática emite una alerta por correo institucional con siete (7) días calendarios de anticipación.

2.3.1 Mantenimiento correctivo a la base de datos

a) En el monitoreo de espacio lógico, se inicia la actividad con la remisión del correo de alerta por espacio lógico, se procede a clasificar el tipo de alerta por Tablespace o diskgroup, las cuales pueden ser:

- Alerta tablespace; las cuales se pueden atender por data o auditoría.

Si se atiende por data, se procede a ampliar la capacidad establecida y se procede a remitir el mensaje de solución de la alerta.
Si se atiende por Auditoría, se procede a realizar el backup de la auditoría, se depura el historial y se remite mensaje de solución de alerta.

- Alerta diskgroup, las cuales se pueden atender por Data Base Information (DBI) y por FRA (Flash Recovery Area).

  Si es por data se debe realizar una petición para crear una nueva LUM (disco), luego se procede a agregar la nueva LUM al diskgroup y se remite el mensaje de solución de la alerta. Caso contrario, si es por FRA se procede a realizar el backup de archivo redo log, luego de ello se depura el archivo redo log y se remite el mensaje de solución de la alerta.

b) En el monitoreo de espacio físico se inicia la actividad por un correo de alerta del filesystem, se procede a verificar qué filesystem disparó la alerta, luego de ello se procede a depurar el archivo de traza con la herramienta del gestor de base de datos (herramienta ADRCI) si con ello el problema no se soluciona, se desarrollan las siguientes acciones:

   - Se procede a buscar las carpetas y LOGs que ocupan mayor tamaño, se realiza el backup de los archivos LOG identificados, luego se accede al archivo LOG y se elimina los datos que se encuentran dentro del log.
   - Si a pesar de ello no se soluciona el problema se procede a realizar una petición para crear una nueva LUM, luego de ello se configura la nueva LUM para filesystem y se procede a cerrar la atención de la alerta.
   - Si el problema se soluciona se comunica el mensaje de solución de la alerta por filesystem.

c) En el caso del monitoreo de ale***rt*** log se inicia la actividad con un correo de alerta de error de log, para lo cual se verifica el código del error, se accede al ***portal*** Oracle support en donde se ingresa el código del error, se verifica las notas técnicas del error y se ejecuta la solución descrita en la nota de la ficha técnica, en el caso que no se haya solucionado el problema se desarrollan las siguientes acciones:

   - Se procede a acceder a la opción de crear caso de soporte, luego el proveedor asignará a un técnico nivel 1 y el ABD se debe contactar con el proveedor para que se conecte vía acceso remoto, el técnico del proveedor indicará una serie de pasos a seguir para solucionar el problema.
   - Si el problema persiste, se escala con otro técnico del siguiente nivel asignado y se brinda el acceso remoto, se siguen los pasos indicados por el técnico y verifica si el problema fue solucionado, si fue solucionado se procede a cerrar la atención.
   - De lo contrario, el técnico del proveedor creará el bug por problema particular, luego de ello recibe la respuesta de la solución del problema y se ejecuta la solución enviada por el proveedor, luego de ello se cierra la atención.

d) En el caso del monitoreo de caducidad de contraseña, se inicia la actividad con un correo del sistema de alerta, se procede a verificar a qué tipo de usuario pertenece la clave a caducar.

   - Si se trata de un usuario final, se asigna nueva clave e informa a los involucrados, luego se cierra la atención.

- Si se trata de una aplicación, se coordina con el personal de desarrollo, se detiene la aplicación, se procede a cambiar la clave en la base de datos, luego de ello se cambia la clave en la aplicación, se reinicia la aplicación y verificar el correcto funcionamiento de la aplicación, ***se registra la nueva clave en la bitácora,*** luego se cierra la atención.
- Si se trata de un esquema, se asigna una nueva clave y se procede a registrar en la bitácora, luego de ello se cierra la atención.

e) Si corresponde a un monitoreo de sesiones, se inicia la actividad por un correo de alerta de sesión de usuario, se cuenta las alertas llegadas por bloqueo de sesión. En base a ello, se revisa si llegó una segunda alerta, se identifica el nombre del equipo desde el cual llegó a acceder el usuario bloqueante y se procede a contactar al usuario del equipo que generó el bloqueo para informar las medidas puede reiniciar el equipo o cerrar la sesión:

- Si se reinicia el equipo se procede a revisar el estado de las sesiones activas, si con ello soluciona el problema, cierra la alerta. De lo contrario, procede a ingresar al administrador de sesiones y fuerza el cierre de sesión del usuario bloqueante, luego cierra la alerta almacenada.
- Si se cierra la sesión, el usuario procede a ingresar al administrador de sesiones y fuerza el cierre de sesión del usuario bloqueante, luego de ello finaliza la actividad.

f) Se procede a realizar el registro del Mantenimiento correctivo de acuerdo al Anexo N° 3 del presente documento.

2.4. Homologar datos de ambientes

Inicia esta actividad a solicitud de un ticket de homologación o por mantenimiento programado. El ABD evalúa si corresponde a un ticket o actividad programada:

a) Si se trata de un ticket, se evalúa si es homologación de metadato, data o algún objeto de la base de datos.
b) Si se trata de un ticket de homologación de metadato, se verifica en el correo, el objeto que se extraerá el metadato, se extraen los metadatos y se envía el script al usuario que realizó la solicitud y se cierra el ticket.
c) Si se trata de un ticket de homologación de objetos o datos, los pasos para la homologación de objetos y datos son los mismos, ambos se inician con la verificación a qué esquema pertenecen los objetos o datos que se van a homologar.
d) Se realiza el backup del esquema y se copia el backup en el ambiente que se especificó en el correo. Se consultan las consideraciones por esquema.
e) Se restaura el backup y se ejecuta los scripts según las consideraciones. Se informa al usuario que realizó el pedido y se cierra el ticket.
f) Si se trata de una actividad programada, se procede a realizar el backup de la base de datos y se copia el backup en los ambientes de calidad y desarrollo.
g) Se revisan las consideraciones a tener por esquema y se restaura el backup.
h) Se procede a ejecutar los scripts según consideraciones y se comunica al área solicitante que la atención fue realizada, luego de ello se cierra la atención.

2.5. Actualizar permisos de usuarios

a) Se inicia con un ticket o solicitud generado por un usuario perteneciente al área de calidad o desarrollo.
b) Después de recepcionar el ticket, se verifica a qué ambiente pertenece el usuario al cual se actualizará el permiso.

c) Si el usuario no pertenece al ambiente de producción solo se procede a realizar la actualización de los permisos.
d) En caso se realice la actualización de permisos de un usuario perteneciente al ambiente de producción, se debe evaluar si es usuario final:
   - En caso de ser usuario final se debe verificar la autorización de un gestor, en caso de no tenerlo no se actualizarán los permisos.
e) En caso de ser un usuario esquema o aplicación, se verifica que cumpla con los requisitos de un pase a producción, para actualizar los permisos se debe seguir lo especificado en *I-PA0304-02 "Operaciones de Tecnologías de la Información".* Después de realizar la actualización de los permisos se procede a informar al usuario que generó la petición y se cierra el ticket o solicitud.

2.6. Restauración de datos de los ambientes

Restauración parcial de data en ambientes de calidad y desarrollo

a. Se inicia con la atención de un ticket o solicitud generada por un usuario perteneciente al área de calidad o desarrollo. En el ticket se debe especificar fecha, esquema y ambiente.
b. Con la información del ticket se busca un backup que cumpla con esas especificaciones.
c. El backup se puede encontrar en dos ubicaciones posibles.
   - La ubicación en disco: se ubica el backup en disco, se restaura el backup en el ambiente especificado y se valida con el usuario la restauración de los datos. Se procede a cerrar el ticket.
   - La ubicación en cinta: comunica, mediante correo institucional, al personal encargado de la administración de las cintas de backup, conforme al instructivo I-OTI-PA0304-2 Operaciones de Tecnologías de la Información.
   - Se le indica la ruta donde debe dejar el backup al administrador de cintas de backups.
d. Se accede a la ruta y se procede a restaurar el backup en el ambiente indicado.
e. Se valida con el usuario la restauración de la información.
f. Se procede a cerrar el ticket.

2.7. Backups de base de datos

2.7.1. Resolución de problema de Backup de base de datos

a) Los backup de la base de datos de los ambientes se generan de manera automática mediante la creación de políticas[6] de backups.
b) Se debe monitorear la ejecución de la política y el estado del backup que se genera.
c) Se inicia cuando se ejecuta la política para generar backup.
d) Se monitorea la ejecución para evitar errores:
   - Si se genera una alerta de error se analiza si se debe volver a generar el backup:
   - Si es un fallo de ***backup*** tipo archivelog: se debe relanzar la política para ejecutar backup ***archivelog***.
   - Si es un fallo de backup full:
     - En caso sea un día no laborable se ejecuta la política de backup full y se almacena el backup.
     - En caso sea un día laborable no se lanza el backup por falta de tiempo y afectación del desempeño de la base de datos.

6 Se refiere a la configuración de las bases de datos para la generación de los tipos y frecuencias de los backups.

e) En caso no se genere ninguna alerta de error en la ejecución se finaliza el backup.
   - Después de obtener los backup de la ejecución de las políticas se evalúa si es fin de mes o no, debido a que el encargado de guardar los backups en cinta presenta un juego de cinta, cada fin de mes Si es fin de mes, se selecciona los backups a guardar en cinta y se deja en una ruta compartida. De lo contrario se mantienen almacenados hasta la fecha indicada de la selección de backup para guardar en cinta. ***Cabe mencionar, que en los backups también se consideran los bancos de datos personales que se encuentren a nivel de base de datos.***

2.7.2. Backup de objetos

Para realizar el backup de objetos se tienen dos formas:

a) Durante un pase a producción donde se modifica el esquema, se crea el comando para generar el backup del objeto, descrito en el documento de pase a producción.

   Se ejecuta el comando que genera el backup y se almacena en la ruta compartida para ser grabado en cinta y se continúa con el pase a producción.

b) Cuando se realiza la solicitud de backup, se recibe el correo institucional y el ticket, se genera y ejecuta el comando para realizar el backup del objeto específico, se almacena el backup, se informa al usuario y se cierra el ticket.

2.8. Procedimiento de Reporte de Auditoría

2.8.1. Procedimiento de Reporte Semestral de Accesos

a) El/La Analista de Administración de base de datos valida que se cumplan con los siguientes requisitos:
   - ✓ Estar en una PC conectada a la Red de OEFA.
   - ✓ Tener configurado un software de administración de base de datos.
   - ✓ Tener TNSNAMES[7] con acceso a las bases de datos.
   - ✓ Tener un usuario de base de datos con acceso de lectura a las vistas y tablas de auditoría.

b) Conectarse a la base de datos y ejecutar el script asociado a este procedimiento.

c) El reporte mostrará las conexiones a la base de datos asociadas, estas conexiones se realizan a través de los aplicativos webs, aplicativos cliente servidor, database links y/o conexión directa.

d) Los reportes de auditorías de accesos contienen las siguientes columnas:
   - ✓ OS_USERNAME: Es el usuario de sistema operativo con el que se realizó la acción que generó una traza de auditoría en la base de datos.
   - ✓ USERNAME: Es el usuario de base de datos con el que se realizó la acción que generó una traza de auditoría en la base de datos.
   - ✓ USERHOST: Es el equipo informático con el que se realizó la acción que generó una traza de auditoría en la base de datos.
   - ✓ TIMESTAMP: Es la fecha y hora en la que se realizó la acción que generó una traza de auditoría en la base de datos.
   - ✓ ACTION_NAME: Es la acción ejecutada que generó una traza de auditoría en la base de datos.

---

7 Es un archivo de configuración que contiene nombres de servicios en red mapeados, a través de los cuales se nos permite acceder.

e) Exportar el reporte y guardarlo en formato Excel.
f) Subir el reporte de auditoría a la ruta compartida que indique el/la Oficial de Seguridad y Confianza Digital.

2.8.2. Procedimiento de Reporte Semestral de Auditoría

a) Se valida que se cumplan con los siguientes requisitos:
   - ✓ Estar en una PC conectada a la Red de OEFA.
   - ✓ Tener configurado un software de administración de base de datos.
   - ✓ Tener TNSNAMES con acceso a las bases de datos.
   - ✓ Tener un usuario de base de datos con acceso de lectura a las vistas y tablas de auditoría.

b) Conectarse a la base de datos y ejecutar el script asociado a este procedimiento.
c) El reporte mostrará la traza de las tablas que tengan auditoría activada para el periodo de un semestre.
d) Este reporte tendrá las siguientes columnas:
   - ✓ OS_USERNAME: Es el usuario de sistema Operativo con el que se realizó la acción que generó una traza de auditoría en la base de datos.
   - ✓ USERNAME: Es el usuario de base de datos con el que se realizó la acción que generó una traza de auditoría en la base de datos.
   - ✓ USERHOST: Es el equipo informático con el que se realizó la acción que generó una traza de auditoría en la base de datos.
   - ✓ TIMESTAMP: Es la fecha y hora en la que se realizó la acción que generó una traza de auditoría en la base de datos.
   - ✓ OWNER: Es el dueño del objeto sobre el que se realizó la acción que generó una traza de auditoría en la base de datos.
   - ✓ OBJ_NAME: Es el objeto sobre el que se realizó la acción que generó una traza de auditoría en la base de datos.
   - ✓ ACTION_NAME: Es la acción ejecutada que generó una traza de auditoría en la base de datos.

e) Exportar el reporte y guardarlo en formato Excel.
f) Subir el reporte de auditoría a la ruta compartida que indique el/la Oficial de Seguridad y Confianza Digital.

2.8.3. Encriptamiento de base de datos

El proceso de encriptamiento de base de datos se realiza a través de la herramienta de Oracle que dispone la entidad, el cual mediante una configuración interna se realiza el proceso al esquema de base de datos, siendo un detalle de los esquemas y al ser información confidencial estas actividades se disponen como responsabilidad de el/la administrador de base de datos.

2.8.4. Bitácora de registro de usuarios

Los administradores de base de datos como parte de sus funciones reciben solicitudes de pases a producción asociados a la capa de base de datos. Antes de ejecutar dicho pase a producción se genera una copia de seguridad de tipo datapump y ya en la ejecución se pueden correr scripts que contengan acciones de tipo INSERT, UPDATE, DELETE, SELECT, entre otros. Asimismo, se realiza en la homologación de esquemas desde el ambiente de producción hacia los ambientes de calidad y/o desarrollo para lo cual también se genera una copia de seguridad de tipo datapump.

De acuerdo a estas acciones se da inicio a las trazas de auditoría de tipo "SELECT" (lectura) debido a que cuando se genera un backup de tipo datapump internamente el motor de base de datos Oracle lee y escanea todas las tablas del esquema y así se generaría un falso positivo para quien ejecutó el backup.
Para llevar el control y seguimiento el/la Administrador/a de Base de Datos debe registrar el Anexo 4- Bitácora de registro de usuarios, donde se registra todos los backups tipo datapump de los esquemas que sean parte de las políticas de auditoría. Asimismo, esta bitácora incluye también los pases a producción en los que se tenga que realizar acciones de SELECT, INSERT, UPDATE, DELETE. El/La gestor/a de infraestructura y comunicaciones verificará mensualmente que la Bitácora sea registrada.

2.8.5. Periodo de retención

a) ***Se establece que el periodo de retención de las auditorías dentro de la base de datos será de un año.***
b) ***Una vez cumplido ese año se genera una copia de seguridad (backup de auditoría), este backup se envía a cinta y luego se procede a depurar la data respaldada.***
c) ***Los backups de auditorías serán los backups full de base de datos obtenidos a las 00:00 horas del primer día del año siguiente. Por ejemplo, el backup full del contenedor ORCL1 del día 01 de enero del 2023 a las 00:00 horas contendrá toda la auditoría del año 2022.***
d) ***Se establece que los backups de auditorías deberán tener un resguardo en cinta por un periodo de tres años.***

2.9. Mantenimiento de auditoría

Se indican los pasos que se deben realizar para ejecutar el mantenimiento de auditoría:

- ✓ ***Ingresar a la ruta donde se encuentran los logs de backup y validar que el backup full haya culminado con éxito.***
- ✓ ***Ingresar a la ruta donde se encuentran los backups y validar que existan los archivos correspondientes.***
- ✓ ***Informar que el backup de auditoría se encuentra en disco (vía correo institucional) y solicitar que sea llevado a cinta.***
- ✓ ***Validar que personal de infraestructura confirme que el backup ha sido llevado a cinta (debe indicar ID de caja e ID de cinta).***
- ✓ ***Informar vía correo institucional que se da inicio a las actividades de mantenimiento anual de auditorías.***
- ✓ ***Obtener el tamaño actual de las auditorías.***
- ✓ ***Ejecutar función propia de la marca Oracle que permita la depuración de auditorías en el periodo de tiempo especificado.***
- ✓ ***Validar que la función se ejecute correctamente, validar que se haya recuperado espacio.***
- ✓ ***Informar vía correo institucional que se culminó las actividades de mantenimiento anual de auditorías.***

2.10. Gestión de cuentas de usuario con privilegios

a) ***Se establece que la vigencia de las contraseñas para usuarios con privilegios es de un año. Esta vigencia se establecerá en el rol "SUPERUSUARIO" a nivel de base de datos.***

b) Se establece que se tendrá una bitácora en la que se registren todos los cambios de contraseña.

c) Siete días antes de cumplido ese año, vía correo electrónico la base de datos alertará la situación, el/la Administrador/a de base de datos informa al gestor de infraestructura y el/la Oficial de Seguridad y Confianza Digital que se debe proceder con el cambio, se programa el mantenimiento para el cambio de contraseña y se genera un ticket.

d) Se realiza el cambio de contraseña y las nuevas contraseñas se registran en la bitácora de contraseña para usuarios con privilegios.

e) Es responsabilidad del gestor de infraestructura verificar que se cumpla con los tiempos establecidos

Anexo N° 1
Crecimiento de la base de datos

			DD/MM/AAAA				DD/MM/AAAA			
Servidor	Nodo 1	Nodo 2	Total Size	Used Space	Free space	% USO	Total Size	Used Space	Free space	% USO
Bases de Datos de Producción										
	TOTAL:		0	0	0		0	0	0	
Diskgroups										

Anexo N° 2:
Solicitud de acceso de base de datos usuarios finales

Colaborador/*a*	:				
Cargo	:		**Área**	:	
Autorizado por	:		**Cargo**	:	
Fecha de Creación	:		**Fecha de Caducidad**	:	
USUARIO/A	:		**Perfil**	:	

TIPO PERMISO	ESQUEMA	OBJETO

Anexo N° 3
Mantenimiento correctivo de base de datos

Servidor	Nodo 1	Nodo 2	Descripción	Fecha de Creación	Tamaño FRA	SGA	PGA	Ubicación Auditorias	Tamaño Redo	GRUPOS	session_cached_cursors open_cursors	CHARACTER SET	Lenguaje
Bases de Datos de Producción													

Anexo N° 4
Bitácora de Registro de Usuarios

GLPI	SOLICITANTE	DESCRIPCIÓN	FECHA EJECUCIÓN	PERSONA EJECUTOR	TIPO DE ACCIÓN	ESQUEMA	OBJETO	POLÍTICA DE AUDITORÍA

Instructivo de operaciones de tecnologías de información

I. OBJETIVO

Establecer las tareas para facilitar la ejecución de las operaciones de tecnologías de la información a nivel de software considerando la atención de los tickets[1] y el monitoreo de la infraestructura.

II. INSTRUCCIONES

Las disposiciones específicas para la atención de los tickets y el monitoreo de las operaciones de software son las siguientes:

2.1. Despliegue de aplicaciones

2.1.1. El despliegue en ambiente de producción - base de datos, inicia con la actividad de tickets emitido por el personal de control de calidad de software, el/la Administrador/a de base de datos (en adelante, ***el ABD***) revisa si la aplicación es nueva o se encuentra ya desplegada en producción.

En relación a las aplicaciones nuevas

2.1.2. Creación de datasource[2]

a) Se inicia con la atención de un ticket generado por las áreas de calidad o desarrollo.
b) Se ingresa al administrador del servidor JBoss[3].
c) Se selecciona la opción datasource.
d) Se selecciona el ambiente donde se creará el datasource.
e) Se crea el datasource con los datos que el/la usuario/a envió en la solicitud de despliegue al ambiente de producción.
f) Los datos necesarios son: nombre, JNDI Name[4], JDBC Driver[5] y cadena de conexión del esquema.
g) Después de haber creado el datasource, se realiza el test de prueba del datasource.
h) Se guarda el nuevo datasource.
i) Se habilita el datasource, en casos de:
- ***Si se creó el datasource durante un despliegue en ambiente de producción, luego se informa a el/la analista de redes o al analista de redes y telecomunicaciones para que continúe con el despliegue en el ambiente de producción de las aplicaciones.***

---

1 Un ticket básicamente es cualquier tipo de consultas, sugerencias o mejoras al producto adquirido, reclamos, pedidos o asesoramiento que como usuario de alguno de nuestros productos o servicios se pueda realizar por la mesa de ayuda.

2 Datasource: representa todo lo relativo a una fuente de datos configurada por el usuario para conectarse a una base de datos.

3 Jboss: es un servidor de aplicaciones Java EE de código abierto implementado en Java puro, más concretamente la especificación Java EE.

4 JNDI Name: es una interfaz de programación (API) que proporciona funcionalidades de nombrado y directorio a las aplicaciones escritas usando Java.

5 Es una API que permite la ejecución de operaciones sobre bases de datos desde el lenguaje de programación Java, independientemente del sistema operativo.

- ***Si se creó por una solicitud o ticket normal, se informa mediante correo institucional al área usuaria y se cierra el ticket.***

2.1.3. Dar de baja a datasource y OJDBC

a) El/La analista programador/a solicita mediante el formato PA0302-F04 solicitud de despliegue la eliminación del datasource antiguo por uno nuevo al analista de calidad de software.
b) Después de haber realizado la modificación y cambio del nuevo datasource de la aplicación y si las pruebas son exitosas, se remite a infraestructura la atención de este cambio de configuración para el aplicativo.

2.1.4. Si la aplicación es nueva, se ejecuta los scripts en el orden descrito en la solicitud de despliegue a producción, se verifica que no tengan objetos descompilados, de requerirse se compilan los objetos en el gestor de base de datos, de lo contrario se inicia con el despliegue de la aplicación.

2.1.5. Posterior a ello, se procede a recibir la confirmación del despliegue y verificar el funcionamiento de la aplicación en el área de calidad; si el despliegue fue exitoso se procede a cerrar la atención del ticket, de lo contrario retorna al ambiente de desarrollo para el levantamiento de observaciones.

En relación a las aplicaciones implementadas

2.1.6. Si la aplicación se encuentra desplegada en el ambiente de producción, se realiza el backup de los esquemas que utiliza la aplicación, se ejecuta los scripts en el orden descrito en el acta de pase a producción; asimismo, se verifica que no tengan objetos descompilados, de requerirse se compilan los objetos en el gestor de base de datos, de lo contrario se inicia el despliegue de la aplicación.

2.1.7. Posterior a ello, se recibe la confirmación del despliegue y verifica el funcionamiento de la aplicación en el área de calidad, si el despliegue fue exitoso se procede a cerrar la atención del ticket, de lo contrario retorna al ambiente de desarrollo para el levantamiento de observaciones.

2.1.8. Si el despliegue de la aplicación está conformado por fuentes y base de datos, antes de realizar las pruebas en calidad, se debe informar, mediante correo institucional, para que se realice el despliegue de las fuentes de acuerdo a lo dispuesto en el Instructivo "*I-OTI-PA0302-1 Instructivo de Desarrollo de Software*".

2.1.9. Culminado el despliegue de las fuentes se procede a la verificación en el ambiente de calidad y se sigue la secuencia de pasos restantes, conforme al Instructivo "*I-OTI-PA0302-1 Instructivo de Desarrollo de Software*".

2.2. Administrar backups

2.2.1. El/La Administrador/a de Redes (en adelante, ***el ADR***) ingresa al software de administración de backups seleccionando el tipo de política de backup que debe crear, sea la política[6] backup full o la backup incremental.

[6] Se refiere a la configuración para la generación de los tipos y frecuencias de los backups.

2.2.2. Luego de crear el tipo de política se selecciona los archivos o servidores que deben ser respaldados y se programa el tiempo de ejecución de la política7.

2.2.3. Posterior a ello, se procede a monitorear el inicio de las políticas y de la generación de la copia de la información en el software de administración de backups y se sincroniza con el servidor de respaldo de la central de datos en la Sede de Chorrillos del OEFA.

2.2.4. Asimismo, se verifica si los datos son críticos, y de corresponder, se procede a respaldar los datos en el centro de datos de respaldo del OEFA, se graba en cintas la información crítica y se registra el backup, luego de ello se culmina la actividad. De lo contrario, se verifica el espacio en el administrador de backups, si hay espacio en disco se almacena los backups (antes de fin de mes), se considera almacenamiento de máquinas virtuales, CMS, base de datos (al final del mes se graba en cinta).

2.2.5. En el caso que se llegue a la fecha límite8, se graba en cinta y se registra el backup, de no encontrarse en fecha límite se mantiene el backup en el appliance hasta la fecha específica de entrega de juegos de cintas y se cierra la atención de generar backups.

Respecto a la entrega de backups

2.2.6. El resguardo de las cintas de backup se desarrolla a través de un servicio brindado por un proveedor.

2.2.7. Diariamente, el proveedor remite una comunicación electrónica indicando los datos del personal que se encargará de recoger las cintas.

a) El/La administrador/a de redes codifica las cintas magnéticas que va entregar.
b) El/La administrador/a de redes selecciona los backups y espera la llegada del personal de la empresa encargado de recoger los backups.
c) El personal de la empresa y personal de la OTI se identifican para asegurar que son las personas autorizadas.
d) El representante del proveedor entrega una caja de seguridad, donde el/la administrador/a de redes guarda las cintas y sella la caja con los precintos.
e) El personal designado por el proveedor recoge las cintas.
f) Completa el formulario de comprobante de servicio.
g) Entrega el comprobante de servicio, con la conformidad, se archiva el comprobante.
h) Se registra el código de precinto relacionado con el código de backups, y se archiva la guía de recepción de las cintas.

Respecto a la recuperación de la información

2.2.8. Si se genera un ticket o una solicitud de restauración de información se desarrollan las siguientes acciones:

a) De la información registrada en el ticket, se verifica el tipo e información que se debe recuperar.

7 Si se trata de la política backup incremental, el tiempo de ejecución es de lunes a jueves de 18:00 a 20:00 horas y de viernes 18:00 a lunes 08:00 am.

8 Antes de fines de mes.

b) Posterior a ello, se localiza en los registros de backup la ubicación de la información, que puede estar almacenada en dispositivos dentro del OEFA o en cintas que se encuentran resguardadas fuera de la Entidad.

2.2.9. Si la información se encuentra registrada en el OEFA, se debe verificar si se encuentra en una cinta o en el appliance9, se realiza lo indicado en el Numeral 3.2.12 del presente instructivo.

2.2.10. Si la información se encuentra registrada fuera del OEFA, se revisa el número de precinto que contiene dentro la caja de seguridad y se solicita vía correo institucional, la caja de seguridad con la cinta. Se confirma la solicitud vía telefónica, se recibe la caja y se verifica que tenga el precinto correcto.

2.2.11. En caso el backup se encuentre en el appliance se debe crear la política de restauración y buscar en el catálogo la aplicación para recuperar la información. En el caso de la cinta solo se debe conectar al equipo computador para que se pueda tener acceso a la información y verificar si tiene o no un catálogo, en caso contar con un catálogo se busca la aplicación de la cual se quiere recuperar la información.

2.2.12. Si la cinta no cuenta con un catálogo se escanea toda la cinta localizando el archivo a recuperar.

2.2.13. Asimismo, se continúa monitoreando el proceso de recuperación de la información en el software para verificar la restauración de la información, confirmando que el usuario pueda acceder a ella y se cierra la solicitud.

2.2.14. Si se ha solicitado las cintas custodiadas fuera del OEFA, se debe regresar la caja, sellar con los precintos, completar los formularios de servicios y contactar con el proveedor para que recojan la caja de seguridad.

Respecto a la Administración del equipo de backup (appliance)

2.2.15. El equipo genera los backups de forma automática, mediante políticas.

2.2.16. La administración comprende: *(i)* el monitoreo del equipo al momento de generar el backup; y, *(ii)* resolver las incidencias que ocurren durante la creación del backup.

2.2.17. En relación al monitoreo de ejecución de políticas de backup, el/la Administrador/a de red desarrolla las siguientes acciones:

a) Monitorea la ejecución de las políticas programadas.
b) Realiza seguimiento a la ejecución de las políticas.
c) Verifica si los backup se generaron correctamente.
d) Monitorea la sincronización de datos críticos con la data center de respaldo.
e) Realiza el monitoreo del tiempo de toda la operación.

2.2.18. En relación a la resolución de incidentes, se desarrollan las siguientes actividades:

a) Se verifica que tipo de incidente ocurrió, pueden ser software o hardware.
b) Se atiende la incidencia y se verifica el estado del equipo.
c) Si todo funciona bien se espera a que se vuelva a generar el backup.

9 Un dispositivo informático es una computadora con software o firmware que está específicamente diseñada para proporcionar un recurso informático específico.

d) En caso de no solucionar el incidente, se procede a contactar al proveedor para la solución del problema.

<u>Respecto al acceso físico al Centro de Datos</u>

a) En el caso que se tengan contratistas que ingresen al centro de datos para el mantenimiento correctivo y/o preventivo, se registra el acceso físico en el documento de visitas que es gestionado por el/la especialista de redes. Asimismo,el ingreso del contratista al centro de datos se realiza en compañía del especialista de infraestructura.
b) En el caso que el personal de infraestructura ingrese al centro de datos este se inscribe por única vez en el equipo biométrico y con ello procede a ingresar al centro de datos; asimismo, la Oficina de Tecnologías de Información tiene un registro de las personas o contratistas que ingresan mediante el software de gestión de accesos.

2.3. Administración de correo *institucional*

2.3.1. Respecto a la solicitud de alta de usuario de un correo institucional, ***el/la Administrador/a de redes*** se desarrollan las siguientes acciones:

a) Se brinda atención de un ticket o correo institucional mediante los cuales se envía un formulario con información sobre el/la usuario/a a quien se le asignará el referido correo.
b) Se verifican los datos del usuario en el Sistema Integrado de recursos humanos (SIA-RRHH)**,** en caso los datos sean incorrectos se realizan las correcciones.
c) Se ingresa al administrador de cuentas de correo y se procede a crear la cuenta, con los datos enviados en la solicitud. Se debe especificar si será correo genérico o no.
d) Se decide qué tipo de cuenta se creará. Si el usuario tiene un cargo directivo, se le asignará una cuenta vault[10], en caso contrario será una cuenta simple.
e) Se completa el formulario con los datos del usuario descritos en la solicitud y se genera la cuenta.
f) Si la solicitud menciona que la cuenta pertenece a un grupo específico.
g) Se envían las credenciales de la cuenta al usuario correspondiente y se cierra la solicitud.

2.3.2. Respecto a la solicitud de baja de usuario de correo institucional, se desarrollan las siguientes acciones:

a) Se atiende la solicitud remitida a través de ticket o correo institucional respecto a la desactivación de la cuenta de correo, a la solicitud se adjunta los datos de la cuenta que será eliminada.
b) Se ingresa al administrador de correo y se procede a desactivar la cuenta.
c) Se cambia la contraseña.
d) Se activa la cuenta.
e) Se ingresa a la cuenta de usuario con la nueva contraseña asignada.
f) Se habilitan las opciones de backup de la cuenta de correo institucional.
g) Se descarga los datos desde la cuenta, mensajes y archivos en la nube. Los mensajes se comprimen en formato PST y los datos de la nube en ZIP.
h) Se graba el backup de los datos de la cuenta en un medio de almacenamiento, siguiendo la instructiva administración de backup.
i) Se suspende la cuenta desde el administrador de cuentas y se elimina la cuenta y se procede a cerrar la solicitud.

[10] Vault permite gestionar la información de los siguientes elementos: Mensajes de Gmail.

2.3.3. Respecto a la solicitud de soporte al servicio de correo institucional, se siguen las siguientes acciones:

a) Se inicia con la recepción de un ticket o solicitud de un usuario.
b) Se verifica si la solicitud será para la restauración del backup o para resolver un problema técnico.
c) Si se trata de una restauración de backup, se verifica si la cuenta tiene un respaldo, en caso de no tenerlo se genera el backup de la cuenta siempre que ésta no haya sido eliminada.
d) Se contacta a el/la usuario/a para informarle el espacio que ocupa los datos, se copia los datos en una carpeta compartida o en un medio de almacenamiento destinado por el usuario.
e) Se debe confirmar con el/la usuario/a si tiene los datos que necesita y procede a cerrar el ticket.
f) Si se trata de un problema técnico, se realiza un diagnóstico del problema, y según ese resultado verificar si el problema se puede solucionar, en caso de tener solución se aplica la solución se informa al usuario y se cierra el ticket.
g) De no tener la solución al problema, se escala el problema al proveedor para que asista en la solución del problema, se aplica la solución del proveedor, se informa al usuario y se cierra el ticket.

2.3.4. Respecto a la solicitud de creación de un grupo de correo institucional, se procede con las siguientes acciones:
a) La atención se inicia con la recepción de un ticket o solicitud, en la solicitud se especifica las características que tendrá el grupo.
b) Se ingresa en el administrador de correo.
c) Se selecciona la opción de crear nuevo grupo.
d) Se asigna el nombre al grupo.
e) Se agrega las cuentas que serán miembros del grupo.
f) Se asignan los permisos que el grupo debe tener.
g) Se cierra el ticket.

2.3.5. Envió de correo masivo
a) Se recibe la solicitud o ticket de correo masivo.
b) Verificar si la petición debe realizarla el área solicitante.
c) Si el mensaje está relacionado con un comunicado o una capacitación se informa al usuario que debe asignar la solicitud a las áreas encargadas como la Oficina de Relaciones Institucionales y Atención a la Ciudadanía (en adelante, ***la ORI***) o la Unidad de Gestión de Recursos Humanos de la Oficina de Administración - URH, de ser ese el caso se envía el correo al área correspondiente y se informa al usuario quien debe realizar el envió de los correos.
d) Si el mensaje se envía por medio del área de operaciones, se debe verificar si el correo tiene la aprobación de la ORI, de no tener su aprobación, se reenvía la solicitud al usuario para que obtengan la aprobación de la ORI.
e) Después de comprobar que cuenta con la aprobación de la ORI, se verifica el asunto que llevará el correo y la hora que debe ser enviado.
f) Se ejecuta la realización del envío masivo de correos.
g) Se informa al usuario de la ejecución de la solicitud y se cierra el ticket.

Las disposiciones específicas para atenciones a tickets y monitoreo de operaciones de software son las siguientes:

a) Alta de usuario de red.

b) Baja de usuario de red.

2.4. Administración de usuarios de red

Respecto a la solicitud de alta de usuario de red

2.4.1. Se inicia la actividad con la atención de ticket emitido por el/la Jefe/a del área correspondiente.

2.4.2. El/La Operador/a de redes, recibe junto con el ticket los datos del nuevo usuario y verifica en la aplicación de SIA-RRHH, que los datos sean los correctos:

- Si los datos no son correctos, se procede a la corrección correspondiente y se realiza lo indicado en el Numeral 2.4.3 del presente instructivo.
- Si los datos son correctos se crea el usuario en la Unidad Organizativa (UO) de Active Directory (AD), correspondiente a su área.

2.4.3. Se procede a crear el usuario en el AD y completar el formulario con los datos del nuevo usuario, luego se procede a revisar los permisos que el/la nuevo/a usuario/a debe tener asignados:

- La petición abarca permisos: se procede a realizar la asignación de los permisos correspondientes descritos en la en el ticket.
- En caso la solicitud abarque acceso a información de los bancos de datos personales del OEFA, se considerará como acceso privilegiado a aquellos perfiles que realicen tratamiento de los datos personales de la Entidad.
- En el caso específico de acceso a los bancos de datos personales de la Entidad, el/la Oficial de Datos Personales es responsable de aprobar los accesos a dicha información.
- Estos accesos se aplican a unidades drive y/o aplicaciones que almacenan datos personales en sus respectivas bases de datos.
- Si el ticket no especifica que se otorgue algún tipo de permiso, se procede a enviar las credenciales a Servicio de TI, para que realice la entrega de las credenciales al usuario.

Baja de usuario de red

2.4.4. La atención se inicia por un ticket o correo institucional con solicitud de atención para baja o eliminación de la cuenta de usuario de red de un usuario especifica.

2.4.5. El/La Operador/a de red recibe el ticket y los datos de el/la usuario/a a dar de baja.

2.4.6. Asimismo, ingresa al AD y procede a buscar a el/la usuario/a.

2.4.7. Posterior a ello, verifica si se le dio un anexo telefónico, si en caso se le asignó un anexo, procede a la eliminación de los datos que aparecen en ese campo.

2.4.8. Se procede a desactivar la cuenta y ubicarla en una UO de cuentas desactivadas; asimismo, la registra en el registro de cuentas desactivadas.

2.5. Administración de accesos a las aplicaciones

2.5.1. Respecto al Sistema de Seguridad - SISEG

El/La Analista de redes y comunicaciones realiza las siguientes actividades:

2.5.1.1. El SISEG es un sistema Single Sign On (inicio de sesión único), conocido también como SSO por sus siglas en inglés, permite a los usuarios tener acceso a múltiples aplicaciones ingresando solo con una cuenta a los diferentes sistemas y recursos.

2.5.1.2. Las aplicaciones que están conectadas con el SISEG son, RIA web, SIIA, Aplicativo de Gestión de Reuniones, REPDIG, AVENP, VIGAMB, SIDECE, Interoperabilidad, SREA, SIPROC, SIGSOL, SISOA, SIJ, SIGI, SIRCOM, SIMUES, SISUD, INAF, SISEFA, Seguimiento de recomendaciones de OCI, Supervisión a Entidades.

2.5.1.3. Para el registro de usuarios, la atención inicia con la recepción de una solicitud o ticket para crear usuario, generada por el/la Jefe/a y Director/a del área usuaria y/o el/la Jefe/a de la Oficina Desconcentrada (OD), cuando ocurre el caso de crear usuarios masivos, se debe realizar la coordinación con el/la Gestor/a de portafolio de proyectos de la Oficina de Tecnologías de la Información.

2.5.1.4. En la opción gestión, ubicada en el módulo usuario dentro del SISEG, se encuentra la opción para crear usuario.

2.5.1.5. Después de seleccionar la opción crear usuario, aparece el formulario el cual se completa con los datos de el/la usuario/a.

2.5.1.6. Si es un/a usuario/a con Contrato Administrativo de Servicios - CAS, Servidores/as Civiles, Secigristas y Practicantes pre profesionales y profesionales, su forma de autenticación es con su usuario de red, de lo contrario se establece una autenticación normal, se genera una clave para que ingrese en el sistema, se debe completar la información de su contrato para que luego quede inhabilitada la cuenta cuando el contrato termina.

2.5.1.7. Se ingresa al módulo perfil, se asignan los roles al nuevo usuario, según la aplicación que especificó en la solicitud y se envían las credenciales al usuario y se cierra el ticket.

2.5.2. Respecto al mantenimiento de cuentas

2.5.2.1. La atención se inicia con la recepción de la solicitud o ticket, se debe especificar los datos de la cuenta.

2.5.2.2. Las acciones de mantenimiento pueden ser:

a) Cambio de contraseña, se tiene que ingresar al módulo usuario en la opción reiniciar usuario, se ingresa la nueva contraseña, se informa al usuario y se cierra el ticket. Esta opción solo aplica a usuarios con autenticación normal.

b) Actualización de permisos, se debe ingresar a la *opción asignar usuarios a rol* ubicada en el módulo perfil. Asimismo, se procede a buscar la aplicación y asignar los roles al usuario, informar al usuario mediante correo institucional, y cerrar el ticket.

2.5.3. En relación al Sistema del Servicio de Información Nacional de Denuncias Ambientales - SINADA

2.5.3.1. Para el registro de usuarios

2.5.3.2. La atención inicia con la recepción de la solicitud por correo institucional o ticket con la autorización de el/la Coordinador/a del SINADA, rol que tendrá el nuevo usuario, la Oficina Desconcentrada (OD) a la cual pertenece y datos del usuario, luego se siguen las siguientes acciones:

a) Se ingresa al administrador del SINADA
b) Se selecciona la opción registrar usuario, ubicado en el módulo usuario.
c) Se completa el formulario con los datos del usuario, la OD a la que pertenece, el rol que tendrá su usuario, entre otros datos que fueron adjuntados en la solicitud.
d) Después de crear el usuario/a, su estado inicial es desactivado, se activa el usuario
e) Luego de activar el usuario se envía las credenciales a el/la usuario/a y se cierra el ticket.

2.5.4. En relación al Sistema de Atención al Ciudadano - SIAC

2.5.4.1. Para el registro de usuario, la atención empieza cuando se recibe el ticket o solicitud por correo institucional, que envía el usuario adjuntando sus datos como: OD o área, perfil que tendrá la cuenta, entre otros datos, para ello se realizan las siguientes acciones:
Se ingresa al módulo de seguridad en la opción mantenimiento de usuario.

a) Se valida si el/la usuario/a existe.
b) Se completa el formulario de nuevo usuario, especificando correctamente el área u OD a la que pertenece, el perfil que tendrá el usuario y la fecha de caducidad de su cuenta.
c) Se verifica si el usuario se creó correctamente.
d) Se envían las credenciales al usuario.
e) Se cierra el ticket.

2.5.4.2. Para dar de baja a un usuario
Se procede con la atención se inicia con una solicitud o un ticket que se envía con los datos adjunto de la cuenta a desactivar, y se desarrollan las actividades siguientes:

a) Se ingresa al módulo de seguridad opción "*mantenimiento de usuario"*.
b) Se valida que el usuario existe en el sistema.
c) Se cambia de estado de activo a inactivo de la cuenta del usuario.
d) Se verifica el estado del usuario, debe estar inactivo.
e) Se notifica mediante correo institucional a el/la usuario/a.
f) Se cierra el ticket.

2.5.5. Respecto al Sistema de Registros de Instrumentos Ambientales - RIA

2.5.5.1. Sobre el registro de usuario se procede con la atención que inicia con la recepción de un ticket o solicitud con un formato adjunto con los datos del nuevo/a usuario/a.

2.5.5.2. Debe tener la autorización de el/la Jefe/a del área y de el/la Director/a, se desarrollan las siguientes acciones:

a) Se ingresa con un usuario administrador al sistema RIA versión escritorio.
b) Se valida si el usuario existe, buscando en la opción persona/entidad ingresando a la opción catálogo.

c) Se crea registro del nuevo usuario, ubicándonos en la opción catálogo y personas.
d) Se completa el formulario con los datos del nuevo usuario y se guarda.
e) Se ingresa al RIA Seguridad, busca al usuario y establece la contraseña de la cuenta.
f) Se asignan permisos al nuevo usuario.
g) Se cierra el ticket y se envían las credenciales.

2.5.6. En relación al Sistema Integrado de Gestión Administrativa (SIGA-OEFA)

2.5.6.1. Sobre el registro de usuario se procede con la atención que inicia con la recepción de un ticket.

2.5.6.2. Ingresar al Sistema de Seguridad Centralizada (SSO) y se desarrollan las siguientes acciones:

a) Se realiza una búsqueda del usuario a crear mediante el número de identificación (DNI).
b) Se valida si el usuario existe, se procede a asignar el permiso *"sigaadm"* que viene a ser un permiso genérico.
c) En caso que el usuario no exista, se procede a registrar primero como Administrado y luego como Usuario en el Sistema de Seguridad Centralizada (SSO), considerando los datos solicitados por el SSO. Luego de ello, se procede a asignar el permiso *"sigaadm"*.

2.5.6.3. Se ingresa al SIGA Cliente, desarrollando las siguientes acciones:

a) Se busca el usuario registrado en el SSO y se crea el usuario en el SIGA Cliente.
b) En base al usuario registrado del SIGA Cliente se ***registran*** los siguientes datos: se le asigna los permisos, se asigna a la Entidad OEFA y a la Oficina(s) que se menciona en la atención.
c) Se procede a guardar, se cierra el ticket y se ***envían*** las credenciales al usuario.

2.5.7. En relación al Sistema de Gestión Electrónica de Documentos (SIGED)

2.5.7.1. Sobre el registro de usuario se procede con la atención que inicia con la recepción de un ticket.

2.5.7.2. Debe tener la autorización del jefe de la Coordinación de Gestión Documental (CGD) y se desarrollan las siguientes acciones:

a) Se ingresa con un usuario administrador al SIGED.
b) Si la atención indica que es usuario nuevo se procede a crear el usuario, asignar el perfil y las bandejas correspondientes.
c) Si la atención indica que es un nuevo cargo del usuario, se procede a actualizar el cargo con la bandeja correspondiente.
d) Si la atención indica que es un cambio de área del usuario, se procede a actualizar la bandeja y crear el cargo en dicha bandeja.
e) Si la atención indica que es una activación temporal del usuario, se procede a reactivar el usuario y sus bandejas cambiando la contraseña del usuario.
f) Si la atención indica que es una baja de usuario, se procede a desactivar el usuario y la bandeja.

g) Se procede a guardar, se cierra el ticket y se envían las credenciales al usuario.

2.6. Baja de aplicaciones

La Oficina de Tecnologías de la Información remite un memorando circular a las áreas usuarias para determinar las aplicaciones que se encuentran en uso y cuales se darán de baja.

- Una vez que se tiene el memorando de respuesta por el área usuaria, el/la Jefe/a de la OTI remite al equipo de infraestructura la lista de las aplicaciones que se darán de baja.
- El equipo de infraestructura crea un backup de la aplicación y a nivel de base de datos, esta información se lleva a cinta tape y se procede a solicitar el almacenamiento con el operador logístico.
- Posterior a ello, se eliminan las rutas públicas de la aplicación y se elimina del servicio la capa aplicación y la capa base de datos.

2.7. Gestión de accesos para usuarios con privilegios (ADMIN, ROOT, SUPERADMIN)

a) Creación de usuarios con acceso privilegiado

El especialista de infraestructura solicita al gestor/a de infraestructura y comunicaciones mediante el formato de Solicitud de acceso privilegiado, los accesos para el cumplimiento de sus funciones, y remite al Oficial de Seguridad y confianza digital (OSCD), para su respectiva validación. Cuando todo se encuentre conforme el OSCD brinda su conformidad con la suscripción del referido formato de solicitud para que se creen los accesos.

El/La Gestor/a de Infraestructura y Comunicaciones con la conformidad del OSCD procede a crear el nuevo usuario y posteriormente el/la Gestor/a de Infraestructura y Comunicaciones registra en la Ficha de Registro de altas, bajas, modificaciones de usuarios con acceso privilegiado. Luego de realizar la creación de usuario, notifica vía correo institucional la creación exitosa al OSCD y al especialista de infraestructura.

b) Modificación de usuarios con acceso privilegiado

La modificación de usuarios con acceso privilegiado se debe realizar haciendo uso del formato de Solicitud de acceso privilegiado (ver Anexo N° 1)

El/La Gestor Infraestructura y Comunicaciones recepciona el formato, firma la solicitud en señal de conformidad y remite al OSCD, para su respectiva validación respecto a los privilegios autorizados y denegados, cuando todo se encuentre conforme el OSCD brinda su conformidad con la suscripción del suscripción mediante una firma en el referido formato de solicitud para que finalmente se modifiquen los accesos.

Con la conformidad del OSCD se procede a modificar los accesos del usuario y posteriormente el/la Gestor/a de infraestructura registra la modificación en la Ficha de Registro de altas, bajas, modificaciones de usuarios con acceso privilegiado.

Luego de realizar la modificación solicitada, el/la Gestor/a de Infraestructura y Comunicaciones debe notificar vía correo institucional la modificación exitosa al OSCD y al especialista de infraestructura.

c) Baja de accesos de usuario privilegiados

Al finalizar un vínculo laboral o prestación de servicios, el/la Gestor/ Infraestructura y Comunicaciones solicitará la baja a través del formato de Solicitud de acceso privilegiado colocando su firma como señal de conformidad.

El/La Gestor/a Infraestructura y Comunicaciones envía el formato al Oficial de Seguridad y confianza digital (OSCD), para su respectiva validación.

Con la conformidad del OSCD el personal de la OTI debe ejecutar las eliminaciones de accesos requeridas.
Luego de realizar la eliminación de accesos solicitada, el/la gestor/a Infraestructura y Comunicaciones debe notificar vía correo institucional la eliminación exitosa al OSCD y al especialista de infraestructura, posteriormente registrarlo en la Ficha de Registro de altas, bajas, modificaciones de usuarios con acceso privilegiado (ver Anexo N° 2).

d) Cambio de claves de usuarios privilegiados
Es responsabilidad del Especialista de Infraestructura realizar los cambios de clave con una frecuencia anual y verificar previamente el impacto que tenga en sus respectivas plataformas e informa, vía correo electrónico, al OSCD.

e) Verificación de cambio de clave de usuarios privilegiados
El/La Oficial de Seguridad de Confianza Digital realiza la verificación anual del cambio de claves por cada plataforma (servidores físicos, virtuales, bases de datos, entre otros).

f) Gestión de las contraseñas de usuarios privilegiados
El/La Gestor de Infraestructura y Comunicaciones mantiene actualizado en un Excel o herramienta para la gestión de usuarios y contraseñas de usuarios con privilegios, esta información es confidencial.

ANEXO N° 1
SOLICITUD DE ACCESO PRIVILEGIADO

1. DATOS DEL USUARIO-

1.1. Solicitud creada por
1.2. Cargo del usuario
1.3. Tipo de relación laboral
○ Trabajador ○ Tercero ○ Empresa

2. DATOS DE ACCESO

2.1. Tipo de acceso
○ Alta ○ Modificación ○ Baja
2.2. Tipo de usuario
○ Administrador ○ Operador ○ Soporte
2.3. Tiempo de vigencia
○ Permanente ○ Temporal ○ Fecha de inicio ○ Fecha de fin
2.4. Sistema de información/ Sistema Operativo, Dispositivo de red
2.5. Justificación del acceso

3. FIRMAS DEL REGISTRO DEL EVENTO

Firma y sello **USUARIO SOLICITANTE** **Fecha:** **Hora:**	Firma y sello **GESTOR/A DE INFRAESTRUCTURA** **Fecha:** **Hora:**	Firma y sello **OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL** **Fecha:** **Hora:**

ANEXO N° 2
REGISTRO DE ALTAS, BAJAS, MODIFICACIONES DE USUARIOS CON ACCESO PRIVILEGIADO

N°	Fecha	Nombre y apellidos del Usuario	Cargo	Nombre de solicitante	Cargo	Tipo de privilegio	Justificación de necesidad de uso	Fecha de caducidad	Autorizado por	Estado de atención
1										
2										
3										

Instructivo de mantenimiento de redes y *comunicaciones*

I. OBJETIVO

Establecer las tareas para facilitar el correcto funcionamiento de las operaciones de tecnologías de la información a nivel de redes y ***comunicaciones*** considerando la atención de tickets y el monitoreo de la infraestructura.

II. INSTRUCCIONES

Las disposiciones específicas para atenciones a tickets y monitoreo de operaciones de hardware son las siguientes:

2.1. ADMINISTRACIÓN DE ANEXO TELEFÓNICO

2.1.1 Actualizar datos de anexo

Inicia la actividad por un ticket virtual para solicitud de anexo telefónico. Se recepciona el ticket para lo cual se solicita los datos de ell/la usuario/a y el área a la cual pertenece.

a) El/La Especialista en Aplicaciones y Telecomunicaciones (EAT) procede a acceder al administrador de equipos telefónicos.
b) Buscar el anexo telefónico a editar, procede a cambiar los datos descritos en el ticket de atención.
c) Verificar que cargo tiene el nuevo usuario y asignar el nuevo número de anexo, Mac del teléfono y datos del pc.
d) Se verifica si tiene nombre genérico, se asigna el nombre genérico, caso contrario se asignará el nombre del usuario solicitado en el ticket.
e) Configurar para salida externa e interna, luego se procede a agregar el anexo en los datos de usuario de red en el Active Directory.
f) Comunicar **al área de** soporte para que realice las pruebas de llamada y verifique que se editó con éxito el número de anexo. Si es conforme, se agrega el número de anexo a la lista de directorios de OEFA y se procede a cerrar el ticket. Caso contrario, se vuelve a editar el anexo y vuelve a iniciar en la actividad b) del presente instructivo.

2.1.2 Trasladar equipo telefónico

a) Se inicia la actividad mediante el ticket virtual de solicitud de anexo, Mac del equipo telefónico, ubicación del equipo, para lo cual se solicita los datos del usuario, área a que pertenece.
b) El equipo telefónico, se reubicará en otro departamento, si es conforme se coordinará con servicios generales para el traslado del equipo y se continúa con el punto c).
c) Conectar equipo en punto de red designado, luego de ello se procede a registrar la Mac del equipo en el puerto del switch.
d) Se procede a editar el anexo y cerrar ticket de atención.

2.1.3 Configurar *UC pone*

a) El EAT, inicia la actividad mediante el ticket de solicitud de actualización de equipo *UC pone* (botonera), para lo cual se revisa la lista de anexos a colocar en la botonera.
b) Verificar si el equipo es compatible con la botonera. Si es compatible, accede al administrador de equipos telefónicos, continúa con la acción c)

del presente instructivo. Caso contrario, procederá a informar que el equipo no es compatible y cierra el ticket de atención.

c) Procede a buscar el anexo telefónico que se actualizará en la lista.
d) Acceder a la opción para agregar la lista de anexos.
e) Asignar a los números de anexo que tendrán cada botón, según plantilla emitida por el/la usuario/a, guardar los cambios realizados.
f) El EAT comunicará a personal de soporte técnico recepcionar los resultados de pruebas del usuario. Se editó con éxito, si es conforme se procede a cerrar el ticket, caso contrario se retorna a la actividad e).

2.1.4 Configurar anexos de las Oficinas Desconcentradas (OD)

a) El EAT, inicia la actividad mediante el ticket de solicitud de solicitud de configuración anexo en OD.
b) Se solicitan los datos de el/la usuario/a de la OD a la cual pertenece.
c) Se procede a contactar con el/la Asistente/a administrativa de la OD.
d) Asistir a el/la colaborador/a de la OD para poder instalar el teléfono y revisar el IP del equipo telefónico.
e) Se solicita el acceso remoto a el/la Asistente administrativa y se procede a actualizar los datos de anexo de la OD. Cerrar ticket de atención.