KR.114

MUNICIPALIDAD PROVINCIAL DE PURUS

Puerto Esperanza – Región Ucayali

ALCALDIA

municipalidadprov.depurus@gmail.com

"AÑO DEL BICENTENARIO DE LA CONSOLIDACION DE NUESTRA INDEPENDENCIA Y DE LA CONMEMORACION DE LAS HEROICAS BATALLAS DE JUNIN Y AYACUCHO"

RESOLUCIÓN DE ALCALDÍA Nº 189-2024-MPP.

Puerto Esperanza, 02 de Octubre del 2024

VISTO:

El Informe Nº 003-2024-MPP-ALC-OTI, de fecha 11 de setiembre del 2024, remitido el jefe encargado de la Oficina de Tecnología de la Información, la Opinión Legal Nº 126-2024-MPP-ALC-GM-GAJ, de fecha 02 de octubre del 2024, remitido por la Gerencia de Asesoría Jurídica, y demás recaudos que contiene;

CONSIDERANDO:

Que, el artículo 194º de la Constitución Política del Estado, en concordancia con el Artículo II del Título Preliminar de la Ley Orgánica de Municipalidades, Ley Nº 27972, los gobiernos locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia. Dicha autonomía radica en la facultad de ejercer actos de gobierno administrativos y de administración con sujeción al ordenamiento jurídico;

Que, el artículo 4º de la Ley Nº 27658, Ley Marco de Modernización de la Gestión Pública, indica que el proceso de modernización de la Gestión del Estado, tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos;

Que, la Política Nacional de Modernización de la Gestión Pública al 2021, aprobada mediante Decreto Supremo Nº 004-2012-PCM, indica en el numeral 4) del artículo 2.3, que la Política Nacional de Modernización de la Gestión Pública, tiene por objetivo general el implementar la gestión por procesos y promover la simplificación administrativa en todas las entidades públicas, a fin de generar resultados positivos en la mejora de los procedimientos y servicios orientados a los ciudadanos y empresas;

Que, a través de la Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 – Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de Seguridad de la Información, Requisitos Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Que, con Resolución Ministerial Nº 320-2021-PCM, se aprueba los "Lineamientos para la gestión de la continuidad operativa y la formulación de los planes de continuidad operativa de las entidades públicas en los tres niveles de gobierno";

Que, mediante Resolución Directoral Nº 022-2022-INACAL/DN de la Dirección de Normalización del Instituto Nacional de Calidad – INACAL, que entre otras normas se aprobó:

- NTP-ISO/IEC 27001:2022: Seguridad de Información, ciberseguridad y protección de la privacidad, Sistemas de Gestión de la Seguridad de la Información, Requisitos. 3ª Edición. Reemplaza a la NTP_ISO/IEC 27001:2024.
- NTP-ISO/IEC 27005:2022: Seguridad de Información, ciberseguridad y protección de la privacidad. Orientación sobre la Gestión de los Riesgos de Seguridad de la Información, 3ª Edición. Reemplaza a la NTP-ISO/IEC 27005:2018;

Que, con Informe Nº 003-2024-MPP-ALC-OTI, de fecha 11 de setiembre del 2024, remitido por el jefe encargado de la Oficina de Tecnología de la Información, eleva a la Gerencia Municipal el proyecto de "Directiva Interna de Normas Técnicas para el Almacenamiento, Respaldo y Restauración de la Información en la Municipalidad Provincial de Purús"; a fin de ser derivado a la Gerencia de Asesoría Jurídica para la opinión legal respectivo;

Que, de acuerdo a lo señalado en los párrafos precedentes, la Gerencia de Asesoría Jurídica, concluye, que de conformidad con las disposiciones legales citadas y el Informe correspondiente, existe la necesidad de contar con una "Directiva Interna de Normas Técnicas para el Almacenamiento, Respaldo y Restauración de la Información en la Municipalidad Provincial de Purús", en virtud a ello, corresponde la aprobación de la misma, de conformidad a los

"AÑO DEL BICENTENARIO DE LA CONSOLIDACION DE NUESTRA INDEPENDENCIA Y DE LA CONMEMORACION DE LAS HEROICAS BATALLAS DE JUNIN Y AYACUCHO"

RESOLUCIÓN DE ALCALDÍA Nº 189-2024-MPP.

considerandos anteriormente expuestos;

Que, estando a las consideraciones expuestas y en uso de las facultades conferidas por el inciso 6) del artículo 20° de la Ley N° 27972, Ley Orgánica de Municipalidades; y, contando con la visaciones de la Gerencia Municipal, Gerencia de Asesoría Jurídica, Gerencia de Planeamiento, Presupuesto, Racionalización y CTI, Oficina de Tecnología de la Información;

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR la Directiva Interna N° 002-2024-MPP-ALC-GM-OTI "**DIRECTIVA INTERNA DE NORMAS TECNICAS PARA EL ALMACENAMIENTO, RESPALDO Y RESTAURACION DE LA INFORMACION EN LA MUNICIPALIDAD PROVINCIAL DE PURUS,** la misma que consta de 16 folios, debidamente rubricados y que forman parte integrante de la presente Resolución, en mérito a lo expuesto en la parte considerativa de la presente Resolución.

ARTICULO SEGUNDO.- DISPONER, el cumplimiento de la presente Resolución a todas la unidades orgánicas de esta entidad edil.

ARTICULO TERCERO.- DEJAR SIN EFECTO, toda norma interna que se oponga a la presente Resolución.

ARTICULO CUARTO.- ENCARGAR, a la Sub Gerencia de Secretaria General cumpla con notificar la presente Resolución y distribución respectiva.

ARTICULO QUINTO.- DISPONER, a la Oficina de Tecnología de la Información, publique la presente Resolución de Alcaldía en el Portal Institucional de la Municipalidad Provincial de Purús.

REGISTRESE, COMUNIQUESE Y CÚMPLASE.

DISTRIBUCIÓN:
GM.
GAJ.
GPPRyCTI
OCI
GODUyR
GDSyE.
GSPyGA.
SGRRHH.
SGPMI.
OTI.
Archivo (02).

Municipalidad Provincial de Purús
Ing. Marcos Pérez Saldaña
Alcalde

DIRECTIVA INTERNA N° 002-2024-MPP-ALC-OTI

DIRECTIVA INTERNA DE NORMAS TÉCNICAS PARA EL ALMACENAMIENTO, RESPALDO Y RESTAURACIÓN DE LA INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DE PURÚS

SUB GERENCIA DE MODERNIZACIÓN INSTITUCIONAL

DIRECTIVA INTERNA Nº 002-2024-MPP-ALC-OTI

Directiva Interna de Normas Técnicas para el Almacenamiento, Respaldo y Restauración de la Información en La Municipalidad Provincial De Purús

I. OBJETIVO

Establecer los lineamientos de almacenamiento y respaldo de la información que permita planificar, ejecutar y controlar las actividades relacionadas al cuidado de la información almacenada y las copias de respaldo de los datos y sistemas informáticos de la Municipalidad Provincial de Purús que propicie la disponibilidad de la Información en caso de fallos o perdidas de datos en las computadoras.

II. FINALIDAD

Asegurar la confidencialidad, integridad y disponibilidad de la información que permita mantener *la comunidad operática de las unidades orgánicas en la Municipalidad Provincial de Purús.*

III. ALCANCE

El presente procedimiento se aplica a los órganos y unidades orgánicas de la Municipalidad Provincial de Purús involucradas en la gestión de respaldo y restauración que requieren ser respaldados, de acuerdo con la importancia o criticidad del mismo, para ser incluidos en los Procedimientos de respaldo.

IV. BASE LEGAL

- Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República.
- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Ley N° 30096, Ley de Delitos Informáticos.
- Ley N° 28716, Ley que regula el control interno de las entidades del Estado.
- Ley N° 2309, Ley que incorpora los Delitos Informáticos al Código Penal.
- Decreto Legislativos N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.
- Resolución Directoral N° 002-2022-INACAL/DN, que aprueba NTP-ISO/IEC 27001:2022. 3ª. Edición.
- Resolución Jefatural N° 286-2002-INEI, que aprueba la Directiva N° 016-2002-INEI/DTPN, "Normas Técnicas para el Almacenamiento y Respaldo de la Información Procesada por las Entidades de la Administración Pública", Firmas y Certificados Digitales.

V. MARCO CONCEPTUAL

5.1. SIGLAS

- **MPP:** Municipalidad Provincial de Purús.
- **OTI:** Oficina de Tecnología de Información.
- **SGTD:** Secretaría de Gobierno y Transformación Digital.

5.2. DEFINICIONES

- **Bases de Datos:** Conjunto de datos que pertenecen al mismo contexto y que están almacenados sistemáticamente para su uso.
- **Carpetas Compartidas:** Espacio de almacenamiento provisto en su red local donde varios ordenadores podrán acceder a los mismos archivos. Incluso, con algunos programas de forma colaborativa (por ejemplo: Word o Excel), sus ordenadores podrán abrir y guardar archivos y carpetas, como si se tratase de una carpeta más de su propio disco duro, pero realmente situada en otro PC, con esquemas de acceso preestablecidos (permisos otorgados), ya sea individual o grupal.
- **Copia de Respaldo – Backup:** Son copias de datos originales disponibles en un soporte magnético o en repositorio digital, con el fin de poder Recuperar la información en caso de pérdida o necesidad de procesamiento de información histórica.
- **Información:** Son los archivos que conforman la data almacenada en un servidor tales como base de datos, archivos, correo electrónico y archivos de repositorio.
- **Información Pública:** Es aquella que ha sido creada u obtenida por las entidades de la administración pública o que posee o que se encuentre bajo control.
- **Política de Retención:** La definición del tiempo de resguardo o retención se efectuará en función de criterios pertinentes tales como; criticidad del sistema, cumplimiento regulatorio, utilidad de la información.
- **Repositorio:** Es un sitio centralizado de recursos informáticos donde se almacena y mantiene información digital, que son accedidos mediante la red de datos según los permisos concedidos al usuario de acuerdo con su perfil. Espacio donde se almacenan las bases de datos.

- **Restauración:** Proceso que hace referencia a la Técnica empleada para recuperar información a partir de una copia de Seguridad (Medio externo); esto aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, aplicación y otros, ataques de virus o Hackers o para atender requerimientos relacionados al Procesamiento de información Histórica.

- **Servidor:** Computadora central en un sistema de red que Provee servicios a otras computadoras

- **Servidor de Archivo (File Server):** Servidor utilizado para almacenar archivos que pueden ser accedidos por los usuarios autorizados de acuerdo con los perfiles que tengan definidos.

- **Unidades de Organización:** Órganos y unidades orgánicas que conforman la Municipalidad Provincial de Purús.

- **Usuario:** Toda persona que cuente con una Computadora Asignada por la Municipalidad Provincial de Purús, con independencia de su régimen laboral o contractual.

VI. RESPONSABILIDADES

- **La Oficina de Tecnología de Información** es responsable de gestionar la seguridad del sistema de información a través de:

  - **Administrador de Redes en TI**

    Perfil Profesional con conocimientos en ciencias de la Computación, Ingeniería de sistemas o Electrónica. Debiendo demostrar habilidades y capacidades en resolución de problemas, capacidad de análisis, pensamiento crítico, gestionar tiempos, trabajar bajo presión y proactividad e iniciativa.

    En cuanto las labores a desempeñar, es el encargado en supervisar los sistemas informáticos, elaborar sus respaldos y verificar las redes de bases de datos; garantizando un óptimo servicio de las telecomunicaciones y conectividad de la entidad.

    Funciones del Administrador de Redes:

    - ✓ Instalar Sistemas de Redes LAN y WAN.
    - ✓ Garantizar el buen Funcionamiento de la Red.

- ✓ Administración de Usuarios.
- ✓ Administración de Programas y Documentación Relacionada.
- ✓ Diagnóstico de Problemas en Redes.
- ✓ Diseño y Elaboración de Soluciones.
- ✓ Maximizar el Rendimiento de Redes LAN y WAN.
- ✓ Mantener los Sistemas de Seguridad Informática.
- ✓ Configurar Routers.
- ✓ Actualizar los Servicios de Datos.

VII. DISPOSICIONES GENERALES

7.1. La información generada y conservada en los equipos informáticos y servidores de datos son de propiedad de la MPP, por lo que es responsabilidad del servidor que realiza su procesamiento velar por la integridad de esta.

7.2. La OTI se encarga de realizar el procedimiento de respaldo de la información y atender las solicitudes de restauración de información formuladas por los usuarios de las unidades de organización de la MPP. Todo sistema de información o aplicación informática que pase a producción debe contener especificaciones técnicas de respaldo de información (ubicación lógica, periodicidad. criticidad), a fin de que la OTI elabore el proceso y programe las tareas para efectuar el respaldo de la información correspondiente.

7.3. La información contenida en las copias de respaldo se mantiene por los periodos correspondientes:

- Diario: Base de Datos, Sistemas de Información.
- Semanal: Sistemas Administrativos y Tributarios.
- Mensual: Sistemas Tributario, SIGA y SIAF.
- Anual: Todos los archivos en general.

7.4. La información contenida en los discos duros de los equipos de cómputo, portátil y equipos similares que tienen asignados los usuarios, no son respaldados por la OTI bajo este procedimiento.

VIII. DISPOSICIONES ESPECIFICAS

8.1. Servidor de Archivos

- La OTI será la encargada de resguardar y administrar el servidor de archivos.
- El Administrador de Redes será el encargado de crear carpetas compartidas y otorgar los permisos de acceso de las unidades orgánicas solicitantes para que estén en disposición de almacenar información que permita mantener la continuidad operativa.

8.2. Recurso compartido en el servidor de archivos

- Solo podrán tener acceso a las carpetas compartidas alojadas en el servidor de archivos, los usuarios que cuenten con la debida autorización.
- Dentro de las carpetas compartidas alojadas en el servidor de archivos, los usuarios tendrán acceso de lectura o lectura y escritura, según corresponda.
- Todas las carpetas compartidas alojadas en el servidor de archivos deberán tener un responsable, que se encargará de realizar las coordinaciones con la OTI en lo que respecta a la carpeta compartida.

8.3. Seguridad Física

- Solo podrán tener acceso a los servidores y bases de datos, los usuarios que cuenten con la debida autorización. Los usuarios solamente tendrán acceso a los servidores y base de datos en forma de lectura o lectura y escritura, según corresponda.
- Todo respaldo realizado deberá contar con un registro en la cual especifique información realizada.
- Los medios magnéticos almacenados, deberán ser resguardados en ambientes que garanticen la preservación de la información, contando con la temperatura y humedad controlada, sistema contra incendio, y los sistemas de seguridad que garanticen su protección ante robos.
- Al almacenar los medios de almacenamientos digitales y/o magnéticos debe hacerlo en cajas especiales de seguridad; las cuales deberán cumplir con las siguientes características:
    - Antiestáticas y resistentes al Impacto.

- Contar con precintos numerados de seguridad.
- Ambiente de uso exclusivo para almacenamiento de medios de almacenamientos digitales y/o magnéticos.

8.4. Respaldo

- Se realizarán copias de seguridad de la información en medios de almacenamiento cada vez que los archivos o base de datos se actualicen, estas copias se podrán efectuar en tres formas:

  a) **Respaldo Total:** Copia completa de todos los archivos en un solo medio de almacenamiento.

  b) **Respaldo Incremental:** Copia de todos los cambios o adiciones que se realizan a determinados archivos cada día.

  c) **Respaldo Diferencial:** Copia de cambios o adiciones que se realizan a determinados archivos respecto al respaldo total, después de cierto periodo de tiempo.

- Los usuarios que tienen asignada una computadora son responsables de realizar el respaldo de la información local. Cada área deberá contar con dispositivos alternos para resguardar documentos que crean conveniente. Adicionalmente cuando algún usuario se retire de un área, se deberá informar al personal de la OTI para generar un respaldo de la información que fue de uso por parte de dicho usuario.

8.5. Restauración de la Información

- La OTI proporcionará a los usuarios que lo requieran, la restauración de los archivos o carpetas digitales que se hayan eliminado o dañado; para tal efecto, el usuario deberá solicitarlo a través de su jefe o encargado, enviando un correo electrónico a la OTI con copia al administrador de redes para su atención, con el nombre de la carpeta o recurso compartido, el nombre de los archivos, carpetas digitales o recursos compartidos a restaurar, la ubicación de los archivos o subcarpetas y de qué fecha aproximada se desea que se haga la restauración. En caso de que no se pueda recuperar la información perdida, la OTI informará las causas al usuario responsable de la carpeta compartida, al jefe o encargado de la Unidad Orgánica.

8.6. Procedimiento de respaldo

- El procedimiento desarrollado estará especificado en el **Anexo 1**, el cual detalla cada uno de los respaldos efectuados por la OTI.

8.7. Usuario de Acceso al Servidor de Base de Datos

- ACCESO, MODIFICACION O ELIMINACION A LA BASE DE DATOS. Deberá solicitarse por correo a la OTI con copia al Administrador de Redes para su atención. En el correo se debe indicar el usuario a crear, modificar o eliminar.
    - En caso de creación: indicar tipo de permiso que deberá tener dicho usuario (solo lectura o lectura y escritura).
    - En caso de modificación: indicar tipo de permiso a modificar.
    - En caso de eliminación, indicar tan solo el usuario.

8.8. Servidor de aplicaciones

- RECURSO COMPARTIDO EN EL SERVIDOR DE APLICACIONES

  Se dispone de un servidor de aplicaciones en el cual se almacenan los archivos de aplicación de los sistemas de la entidad, debiendo tomar en cuenta lo siguiente:

  a) Solo podrán tener acceso a los recursos compartidos alojados en el servidor de aplicaciones los usuarios que cuenten con la debida autorización.

  b) Dentro de los recursos compartidos alojados en el servidor de aplicaciones, los usuarios tendrán acceso de lectura o lectura y escritura, según corresponda.

  c) Los permisos de acceso podrán ser otorgados y/o retirados previa coordinación y autorización del responsable de la OTI.

- INFORMACION ALMACENADA EN EL RECURSO COMPARTIDO EN EL SERVIDOR DE APLICACIONES.

  Los usuarios con acceso a un recurso compartido alojado en el servidor de aplicaciones son responsables de:

a) Almacenar únicamente información relacionada con la labor o servicio que realiza.

b) Conservar la integridad y confidencialidad de la información compartida.

IX. DISPOSICIONES FINALES

9.1. La Oficina de Tecnología de Información es responsable, en el ámbito de su competencia, de cumplir y hacer cumplir las disposiciones contenidas en el presente documento.

9.2. La Oficina de Tecnología de Información debe gestionar en su presupuesto anual los recursos para adquirir, implementar y mantener el proceso de gestión de copias de respaldo de la información de la Municipalidad Provincial de Purús.

X. ANEXOS

- ✓ Anexo 1 - Procedimiento de respaldos
- ✓ Anexo 2 - Programa de respaldo de la información
- ✓ Anexo 3 - Registro de respaldo de la información
- ✓ Anexo 4 - Programa de restauración de la Información
- ✓ Anexo 5 - Acta de restauración

Anexo 1 - Procedimiento de respaldos

N°	Descripción de la Actividad
1	Según Corresponda: - Necesidad de respaldar los activos de información Críticos: Identificar Previamente los activos de información que requieren ser respaldados, de acuerdo con la importancia o criticidad del mismo, para ser incluidos en los Procedimientos de respaldo (base de datos, correo electrónico, copia de seguridad de los equipos, servidores, aplicaciones, servicios, entre otros). Continuar con la Actividad 2. - *Necesidad de restaurar los activos de información críticos: Continuar con la Actividad 9.*
2	Registrar los datos solicitados en el "Programa de Respaldo de la información" (**Anexo N° 02**) – Tipo de respaldo que se va a utilizar, en la planificación: • Respaldo Full. • Respaldo Incremental. - Frecuencia en la cual se debe de crear el respaldo respectivo. - Origen de la información a respaldar: • De donde proviene la información ya sea de un equipo o servicio. • Dirección IP. • La Ruta. • El ambiente en que trabaja. - Destino de la información a respaldar - Nombre de Job. - *Retención.* - Observaciones.
3	Ejecutar el respaldo de la información, realizando las siguientes acciones: - Acceder al sistema de copias de respaldo. - Crear la tarea Programada de copia de respaldo. • Indicar el recurso al que se va hacer el Backup y la Ruta. • Tipo de Respaldo y Frecuencia. - Ejecutar las tareas programadas. • Tarea ejecutada automáticamente por el software de Backup. - Copiar el Backup realizado a Diario, Semanal, Mensual. Nota: Los datos grabados se deben verificar al finalizar la copia, debido a que estos pueden presentar errores.
4	Revisar si la ejecución del respaldo de la información se realizó correctamente. ¿Es conforme? - Sí: continua en la actividad **6.** - No: continua en la actividad **5.**

5	Revisar el logro generado del respaldo de la información para identificar y solucionar el problema. ¿Se solucionó? - Sí: Ir a la actividad 3. - No: Escalar al proveedor para que solucione el problema identificado. Fin del procedimiento.
6	Registrar el respaldo de la información en el "Registro de respaldo de la información" **(Anexo N° 03):** - Equipo / Servicio. - Fecha y Hora de inicio de la creación del respaldo a registrar. - Fecha y Hora de finalización del proceso de creación del respaldo. - Nombre de JOB. - Estado en que se encuentra el respaldo realizado. - Responsable, encargado de realizar el respaldo. - Nombre del medio en que se guarda la copia de respaldo: Almacenamiento en la Nube. - Observaciones que se tengan, realizando la copia de respaldo.
7	Agregar en el registro de respaldo **(Anexo N° 04),** la siguiente información: - Código. - Fecha de Ingreso. - Fecha de Salida. - Contenido. - Periodo de Retención. - Fecha de Custodia.
8	Enviar correo electrónico del resultado de respaldo de la información al jefe de OTI. Fin del procedimiento.
9	Programar las fechas de restauraciones de la información y registrar los datos en el "Programa de restauración de la información" **(Anexo N° 05),** considerando lo siguiente: - Fecha para ejecución de restauración. - Fuente a restaurar (servidor, base de datos, servicio o aplicación). - Responsable de ejecutar la restauración. - Respaldo a restaurar. - Fuente de la información: • Servidor de Backup. - Método de restauración:

	• Restauración Full. • Restauración Incremental.
10	Revisar y Aprobar el "Programa de restauración de la información".
11	Identificar lo programado a restaurar.
12	Revisar si la ejecución de la restauración se realizó de la manera correcta. ¿Es correcta? - Sí: Continua en la actividad **14.** - No: Continua en la actividad **13.**
13	Revisar el registro de respaldos y seleccionar el backup anterior para restaurar. Ir a la actividad **11.**
14	Registrar la restauración de la información en el Acta de restauración **(Anexo N° 05),** incluyendo la siguiente información: - Fecha de la restauración. - Hora de inicio del proceso de restauración. - Hora de finalización del proceso de restauración. - Servidor / Aplicación. - Respaldo a restaurar. - Servidor destino – Fuente (Almacenamiento en la Nube). - Actividades realizadas. - Resultados de la restauración.
15	Enviar correo electrónico del resultado de restauración del jefe de OTI.
FIN DEL PROCEDIMIENTO	

Anexo 2 - Programa de respaldo de la información

Programación		Origen de la información por respaldar				Destino de la información a respaldar	Nombre del job	Retención	Observaciones
Tipo de Respaldo	Frecuencia	Equipo / Servicio	IP	Ruta	Ambiente	Ruta			

MUNICIPALIDAD PROVINCIAL DE PURUS · OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN · V° B°

MUNICIPALIDAD PROVINCIAL DE PURUS · SUB GERENCIA DE MODERNIZACIÓN INSTITUCIONAL · V° B°

Anexo 3 - Registro de respaldo de la información

Equipo / Servicio	Fecha y Hora Inicio.	Fecha y Hora Fin.	Nombre del JOB	Estado	Responsable	Nombre Dispositivo de Respaldo	Observaciones

Anexo 4 - Programa de restauración de la Información

Fecha	Servidor / Aplicación	Responsable	Respaldo por Restaurar	Servidor Destino	Fuente (servidor de Backup)	Método Restauración (Full, Incremental)

MUNICIPALIDAD PROVINCIAL DE PURÚS OTI V° B° OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

MUNICIPALIDAD PROVINCIAL DE PURÚS V° B° SUB GERENCIA DE MODERNIZACIÓN INSTITUCIONAL

Anexo 5 - Acta de restauración

Fecha:			
Hora Inicio:		**Hora Fin:**	

Servidor / Aplicación	Respaldo por Restaurar	Servidor Destino	Fuente (Servidor de Backup)

ACTIVIDADES REALIZADAS

MUNICIPALIDAD PROVINCIAL DE PURÚS OTI V° B° OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN

RESULTADOS

MUNICIPALIDAD PROVINCIAL DE PURÚS SUB GERENCIA DE MODERNIZACIÓN V° B°

FIRMAS

RESPONSABLE 1

RESPONSABLE 2