REPÚBLICA DEL PERÚ

REGIÓN PUNO

RESOLUCIÓN GERENCIAL GENERAL REGIONAL

Nº 238 -2024-GGR-GR PUNO

Puno, ... 24 SEP. 2024 .....

EL GERENTE GENERAL REGIONAL DEL GOBIERNO REGIONAL PUNO

Vistos, el expediente GGR00020240001021, sobre aprobación del PLAN DE GENERACIÓN DE COPIAS DE RESPALDO (BACKUP) 2024-2025;

CONSIDERANDO:

Que, el Jefe de la Oficina de Tecnologías de la Información, ha emitido el Informe N° 000142-2024-GRP/OTI de fecha 29 de agosto del 2024, dirigido al Gerente General Regional, para elevar la propuesta del PLAN DE GENERACIÓN DE COPIAS DE RESPALDO (BACKUP) 2024-2025;

Que, el objetivo del Plan mencionado en considerando precedente es *"Diseñar e implementar un plan integral de continuidad y recuperación de incidentes para el Gobierno Regional Puno, que incluya la generación de copias de respaldo de información de servidores, aplicaciones y bases de datos"*, en la introducción se indica que *"El presente documento define las actividades relacionadas con la generación de copia de respaldo (backup) de los sistemas de información del Gobierno Regional Puno… Estos proporcionan lineamientos mínimos para proteger y garantizar que los activos críticos de la entidad (servidores locales, infraestructura en nube, aplicaciones, código fuente, bases de datos y otros activos de tecnologías de la información), se mantengan respaldadas y sean fácilmente recuperables cuando sea necesario, manteniendo su integridad, confidencialidad y disponibilidad…"*; y

Estando al Informe N° 000142-2024-GRP/OTI e Informe N° 000142-2024-GRP/OTI del Jefe de la Oficina de Tecnologías de la Información, Informe N° 000271-2024-GRP/SGP de la Sub Gerencia de Planeamiento, Informe N° 00978-2024-GRP/GRPPM de la Gerencia Regional de Planeamiento, Presupuesto y Modernización, y Proveído 026040-2024-GRP/GGR de Gerencia General Regional;

En el marco de lo establecido por la Resolución Ejecutiva Regional Nº 076-2023-GR PUNO/GR;

SE RESUELVE:

ARTÍCULO ÚNICO.- APROBAR el PLAN DE GENERACIÓN DE COPIAS DE RESPALDO (BACKUP) 2024-2025, que en nueve (09) rubros, y en doce (12) folios, forma parte de la presente resolución.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

GOBIERNO REGIONAL V°B° Gerencia General Regional PUNO

JUAN OSCAR MACEDO CARDENAS
GERENTE GENERAL REGIONAL

GOBIERNO REGIONAL PUNO

PLAN DE GENERACIÓN DE COPIAS DE RESPALDO (BACKUP)

2024-2025

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

INDICE

ÍNDICE DE TABLAS

I. INTRODUCCIÓN

El presente documento define las actividades relacionadas con la generación de copias de respaldo (backup) de los sistemas de información del Gobierno Regional Puno, aplicando las mejores prácticas y estándares de copias de seguridad. Estos proporcionan lineamientos mínimos para proteger y garantizar que los activos críticos de la entidad (servidores locales, infraestructura en nube, aplicaciones, código fuente, bases de datos y otros activos de tecnologías de la información), se mantengan respaldados y sean fácilmente recuperables cuando sea necesario, manteniendo su integridad, confidencialidad y disponibilidad.

En este contexto, es importante resaltar que, para la correcta ejecución de los lineamientos establecidos en la generación de las copias de respaldo de los activos críticos aquí descritos, se deben analizar detenidamente las políticas de operación definidas dentro del procedimiento de copias de respaldo del Gobierno Regional Puno, como premisa para la aplicación de las actividades relacionadas en este documento.

El propósito principal es establecer e implementar estrategias que permitan generar, recuperar y mantener copias exactas de la información crítica y datos vitales almacenados en los componentes tecnológicos del centro de datos del Gobierno Regional Puno, en caso de presentarse un incidente de seguridad o una falla operativa en alguno de los equipos o componentes tecnológicos, garantizando así su restauración y la recuperación de la entidad ante tales eventualidades.

Dentro de las estrategias principales definidas en el presente documento se encuentran:

- Proporcionar un modelo operativo estándar para las copias de seguridad de la información de la entidad.
- Establecer un estándar para el etiquetado de los medios de copias de seguridad.
- Definir un estándar para el almacenamiento y la recuperación de la información.
- Generar lineamientos claros para la creación de copias de seguridad.

II. OBJETIVO

Diseñar e implementar un plan integral de continuidad y recuperación de incidentes para el Gobierno Regional Puno, que incluya la generación de copias de respaldo de información de servidores, aplicaciones y bases de datos.

III. ALCANCE

Inicia con la planeación de la generación del respaldo de la información almacenada bajo la infraestructura del Gobierno Regional Puno, y finaliza con la ejecución y verificación de las copias de seguridad. Estos lineamientos aplican para los siguientes activos de información:

- Bases de datos en producción
- Código fuente
- Activos de información
- Configuración de infraestructura
- Configuración de redes
- File Server
- Directorio activo
- Correo electrónico

Las actividades relacionadas con la ejecución de copias de respaldo, terminan con la verificación del backup y posterior custodia de dichas copias de seguridad de acuerdo con los lineamientos establecidos por gestión documental.

IV. BASE LEGAL

- Ley N° 27658: Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 27867: Ley orgánica de Gobiernos Regionales
- Resolución Ministerial N° 004-2016-pcm: Aprueban 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.
- Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 085-2023-PCM, que aprueba la Política Nacional de Transformación Digital al 2030
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.

Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.

Decreto Legislativo N° 1246, que aprueba diversas medidas de simplificación administrativa y Decreto Supremo N° 016-2020-PCM que amplía los servicios de información en el marco del Decreto Legislativo N°1246, del Decreto Legislativo N° 1427 y del Plan Nacional de Competitividad y Productividad.

- Resolución Ministerial N° 087-2019-PCM, mediante el cual se Aprueban disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.

V. DEFINICIONES

Backup o copia de respaldo:
Es una copia de seguridad de los archivos, aplicaciones y bases de datos originales, disponibles en unidades de almacenamiento, con el fin de poder recuperar la información en caso de un daño, borrado accidental, accidente imprevisto o pérdidas. Es conveniente realizar copias de seguridad y verificación de las mismas a intervalos temporales fijos (diario, semanal, mensual, por ejemplo), en función de la importancia de los datos manejados o la criticidad que ello represente para garantizar la continuidad de servicio de la entidad. Estas copias son útiles ante de diferentes eventos tales como: Catástrofes naturales, informáticas o ataque informáticos.

Base de Datos:
Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente. En una base de datos, la información se organiza en campos y registros. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo.

Data center:
Ambiente donde se almacena y/o procesa información y/o datos de la entidad, es empleado para albergar los sistemas de información y/o componentes asociados, como telecomunicaciones y los sistemas de almacenamiento donde generalmente incluyen fuentes de alimentación redundante o de respaldo, para permitir que los equipos tengan el mejor nivel de rendimiento con la máxima disponibilidad de los sistemas.

Resguardo externo:
Resguardo realizado por un proveedor contratado por la institución, para brindar el servicio de custodia y almacenamiento externo de las cintas magnéticas de backup, bajo estándares recomendados por el fabricante.

Resguardo interno:
Ambiente de custodia de los medios de almacenamiento, ubicado dentro del Data Center o en un ambiente cercano a este.

Contingencia:
Conjunto de procedimientos de recuperación. Las acciones a contemplar aplican para Antes-Durante- Después con el fin de reducir las pérdidas de información generadas por eventos inesperados.

Plan de Contingencia:
Procedimientos alternativos de una entidad cuyo fin es permitir el normal funcionamiento de esta y garantizar la continuidad de las operaciones, aun cuando algunas de sus funciones se vean afectadas por un accidente interno o externo.

Recuperación:
Hace referencia a las técnicas empleadas para recuperar archivos a partir de una copia de seguridad (medio externo). Esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.

Restauración:
Volver a poner algo en el estado inicial. Una Base de Datos se restaura en otro dispositivo después de un desastre.

Directorio Activo:
Servicios que se ejecutan en Windows Server para administrar permisos y acceso a recursos en red. El directorio activo almacena datos como objetos. Un objeto es un elemento único, como un usuario, grupo, aplicación o dispositivo, como una impresora.

Activos de información:
Volumen en donde se encuentran archivos que hacen parte integral de una aplicación (jpg, pdf, docx, pptx, xlsx).

Repositorio:
Ambiente de respaldo donde se almacena, organiza, mantiene y difunde información como archivos informáticos, base de datos, entre otros. Los datos almacenados en un repositorio pueden distribuirse a través de una red informática, como Internet, o de un medio físico, como un disco compacto.

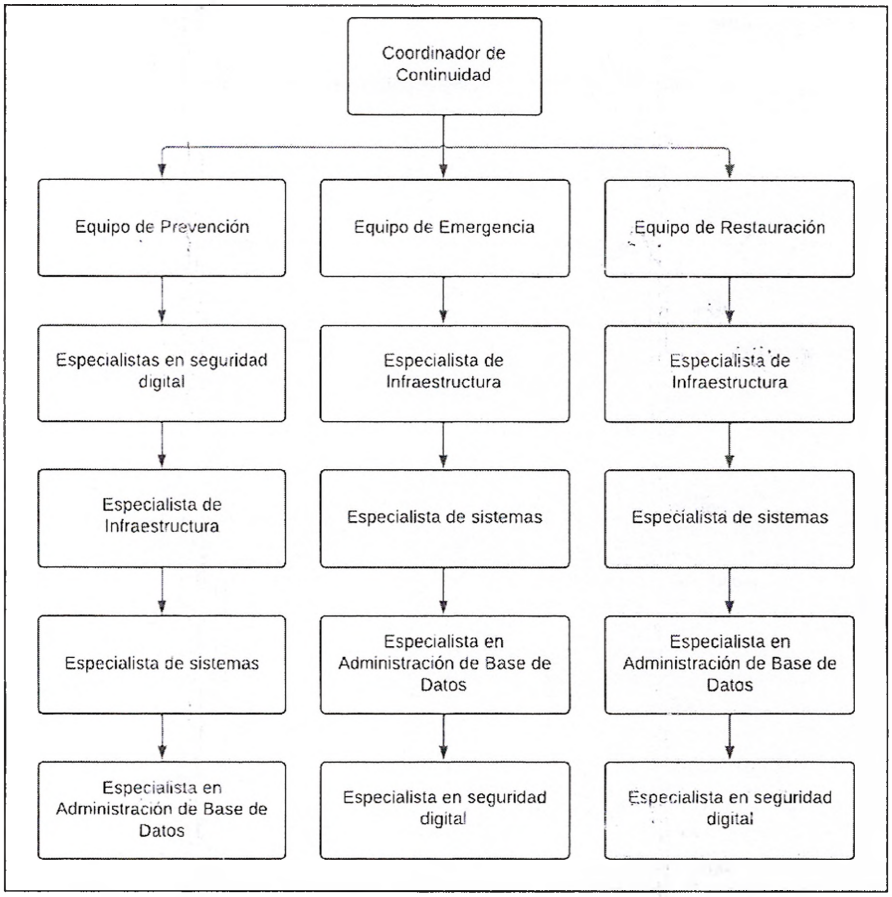
File Server:
Instancia de servidor central de una red de ordenadores que permite a los clientes conectados acceder a sus propios recursos de almacenamiento.

VI. REALIZACIÓN DE COPIAS DE SEGURIDAD DE DATOS

Las copias de seguridad de los datos se programarán diaria, semanal y mensualmente según la naturaleza de la copia de seguridad. Los administradores de datos deben utilizar la tecnología de respaldo de datos aprobada para preparar, programar, ejecutar y verificar respaldos. Las copias de seguridad se pueden realizar en recursos de almacenamiento local (por ejemplo, disco, en la nube, RAID, otros) localmente o en ubicaciones seguras fuera del Gobierno Regional Puno (por ejemplo, proveedores de servicios de copia de seguridad de datos en la nube, proveedores de copia de seguridad como servicio) aprobados por la OTI.

VII. ROLES Y RESPONSABLES

Establecemos los roles y responsables a partir de los equipos formados en el Plan de Contingencia de Tecnologías de la Información del Gobierno Regional Puno.



GOBIERNO REGIONAL V° B° OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - PUNO -

7.1. Coordinador de Continuidad

El Coordinador de continuidad es el jefe de la Oficina OTI. Es responsable de liderar las estrategias de respaldo de datos estén alineadas con los objetivos organizacionales y las normativas de seguridad de la información. Son sus responsabilidades:

- Definir la política de backup y estrategias de recuperación de datos.
- Coordinar con otros departamentos para asegurar la integración de las soluciones de backup.
- Garantizar la disponibilidad de recursos y presupuesto para implementar y mantener soluciones de backup adecuadas.
- Supervisar todo el proceso de respaldo de datos, incluyendo la planificación, ejecución, verificación y restauración de las copias de seguridad.
- Asegurarse de que los equipos designados cumplan con los tiempos establecidos para las copias de respaldo y las pruebas de restauración, además de coordinar con los equipos en caso de fallos o incidentes.

7.2. Equipo de Prevención

El equipo de prevención de TI es responsable de diseñar, implementar, mantener y gestionar la infraestructura tecnológica necesaria para soportar las operaciones de back-up y recuperación de datos de la organización. Son sus responsabilidades:

- Programar y ejecutar las copias de seguridad según los requerimientos definidos.
- Mantener y monitorear la infraestructura de almacenamiento, servidores y redes necesarios para respaldar los datos de manera segura.

- Realizar pruebas de recuperación y troubleshooting para garantizar la integridad de los respaldos.

Especialistas en Seguridad Digital:
Nuevas responsabilidades: Garantizar que las copias de seguridad estén protegidas con los métodos de cifrado correspondientes, y que se cumplan todas las normativas de seguridad en la gestión de las copias.

Especialista de Infraestructura:
Nuevas responsabilidades: Monitorear y asegurar que los servidores y almacenamiento tengan la capacidad suficiente para soportar las copias de seguridad. Coordinar con el equipo de infraestructura en caso de necesidad de escalamiento de recursos.

Especialista de Sistemas:
Nuevas responsabilidades: Colaborar en la automatización del proceso de backups y en la configuración de alertas automáticas en caso de fallos. Garantizar que los sistemas operen de manera óptima durante los procesos de copia de seguridad.

Especialista en Administración de Base de Datos:
Nuevas responsabilidades: Asegurarse de que las bases de datos críticas tengan copias de respaldo regulares y se integren correctamente con los sistemas de restauración en caso de un incidente.

7.3. Equipo de Restauración.

El equipo de restauración de TI es responsable de proteger la integridad, confidencialidad y disponibilidad de los datos durante el proceso de backup y recuperación. Este equipo implementa políticas y procedimientos de seguridad para mitigar riesgos asociados con la manipulación y almacenamiento de datos sensibles. Son sus responsabilidades:

- Validar la integridad y seguridad de los respaldos de datos.
- Implementar medidas de seguridad para proteger los datos durante la transferencia y almacenamiento.
- Participar en la planificación y ejecución de estrategias de recuperación ante desastres y pruebas de continuidad operativa.
- Ejecutar pruebas regulares de restauración de las copias de seguridad y asegurar que todos los datos críticos puedan ser recuperados sin problemas.

Especialista de Infraestructura:
Verificar que los recursos de almacenamiento y servidores estén disponibles y correctamente configurados para soportar restauraciones.

Especialista de Sistemas:
Asegurarse de que los sistemas restaurados estén operando correctamente y que la funcionalidad se haya restaurado por completo.

Especialista en Administración de Base de Datos:
Probar la restauración de bases de datos de manera regular y verificar la integridad de los datos tras las pruebas de restauración.

Especialista en Seguridad Digital:
Garantizar que las copias de seguridad restauradas cumplan con los estándares de seguridad y estén protegidas adecuadamente después de la recuperación.

7.4. Equipo de Emergencia

El equipo de emergencia es el encargado de gestionar la respuesta en situaciones críticas. Este equipo debe coordinar la ejecución de restauraciones rápidas de datos en caso de fallos en los sistemas o pérdida de información o ocurra cualquier otro evento desafortunado que atente contra la información, asegurando que se prioricen las restauraciones de datos críticos.

Especialista de Infraestructura:
Nuevas responsabilidades: Gestionar la disponibilidad de servidores y recursos para restaurar los sistemas, minimizando el tiempo de inactividad durante una emergencia.

Especialista de Sistemas:
Nuevas responsabilidades: Ejecutar los procesos de restauración de aplicaciones y sistemas en coordinación con el especialista de infraestructura.

Especialista en Administración de Base de Datos:
Nuevas responsabilidades: Coordinar la restauración de bases de datos críticas en el menor tiempo posible, verificando la integridad de los datos recuperados.

Especialista en Seguridad Digital:
Nuevas responsabilidades: Asegurarse de que los procesos de restauración sean seguros y que los datos restaurados no comprometan la seguridad de los sistemas.

7.5. Cuadro de actividades

Basado en la Matriz RACI (Responsible, Accountable, Contribute, and Inform), los siguientes grupos y/o personas son identificados para asegurar que la información sea respaldada y almacenados correctamente.

Tareas/Responsabilidades	Coordinador de Continuidad	Equipo de Prevención	Equipo de Emergencia	Equipo de Restauración
Supervisión del proceso de respaldo de datos	A	I	I	I
Realización de las copias de seguridad	R	R	C	I
Verificación de la capacidad del sistema para realizar backups	I	R	I	I
Automatización de procesos de backup	I	C	C	I
Configuración de alertas en caso de fallos en backups	I	C	I	I
Protección de backups con cifrado	I	C	I	I
Pruebas de restauración de backups	A	I	C	R
Restauración de sistemas y bases de datos críticos	A	I	R	R
Monitoreo de la capacidad de almacenamiento y servidores	I	R	C	C
Verificación de la integridad de los datos restaurados	A	I	C	R
Garantía de seguridad post-restauración	I	C	C	R

Tabla: Matriz RACI, cuadro de actividades

Referencia de la Matriz RACI:

- R (Responsable): La persona o equipo que lleva a cabo la tarea.
- A (Aprobador): La persona que toma las decisiones finales y aprueba los resultados.
- C (Consultado): Aquellos que son consultados antes de tomar una decisión o ejecutar una acción.
- I (Informado): Aquellos que deben ser informados sobre el progreso o los resultados de la tarea.

VIII. DESCRIPCIONES DEL PLAN

El objetivo de este documento del Plan de generación de copias de respaldo es definir e implementar las acciones necesarias para crear, recuperar y conservar las copias de la información producida por la entidad, asegurando el cumplimiento de sus funciones y misiones. En caso de un desastre, es crucial que la información esté accesible en una ubicación alternativa para su recuperación. Este documento especifica las actividades que la entidad debe realizar para adherirse a los estándares y normativas aplicables al procesamiento de respaldos.

- Planeación: Establecer cada una de las estrategias y lineamientos para garantizar la realización de las copias de respaldo, así como sus respectivas pruebas de restauración y almacenamiento.
- Hacer: Desarrollar cada una de las actividades contempladas en el proceso de Backup. Realizar actividades para la recuperación de información cuando sea necesario.
- Verificación: Supervisión de los BKF o Backup Datos por tamaño y fecha de modificación y registro diario en la bitácora de control de Backups.
- Actuar: Hacer seguimiento al proceso de Backups, mediante la ejecución de manera periódica de pruebas de restauración de algunas copias de backup para garantizar su correcto funcionamiento. En caso que los backups no se estén realizando correctamente se deberá informar inmediatamente al responsable de esta actividad para tomar los correctivos necesarios.

IX. PLAN DE GENERACIÓN DE COPIAS DE RESPALDO

En el presente apartado se describen las diferentes estrategias para garantizar el correcto funcionamiento del esquema de backups, definiendo los diferentes escenarios que hacen parte de la arquitectura tecnológica actual de la entidad, los cuales son necesarios para proteger y respaldar los activos de información y de esta manera garantizar fácilmente su recuperación en el momento de ser requerido.

FICHA 01: DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO SERVIDORES VIRTUALES	
ACTIVIDADES ESENCIALES	• Realizar copias de respaldo de los servidores virtuales que están en producción, de una manera óptima y práctica, para su posterior almacenamiento; por fechas, nombres y demás disposiciones para restauraciones programadas y de emergencia. • Es necesario realizar una copia de seguridad de las máquinas virtuales en producción, que contenga la estructura en hardware y software virtual, tales como Memoria, Procesamiento, Dispositivos de red, Discos duros virtuales, entre otros.
TIPO	Servidores Nube (cloud computing)
PROCEDIMIENTO	• Realizar las copias de seguridad backup cada un (01) día o máximo cada dos (02) días • Por medio de herramientas de copias de respaldo, se realiza la integración con la infraestructura Virtual correspondiente a los servidores nube, y se seleccionan los que correspondan a producción, entre ellos: MV de Aplicaciones, MV de Base de Datos, SERVIDOR DE ARCHIVOS FILE SERVER y MV que correspondan al funcionamiento de la infraestructura tecnológica, entre otros que sean previamente solicitados. • Mediante la herramienta generadora de copias de respaldo, se realiza una programación de una tarea donde se ejecutarán periódicamente dos tipos de Backups: ✓ Backup Tipo Full: Este tipo de backup contendrá una copia íntegra del 100% de la Máquina virtual previamente seleccionada. Este tipo de respaldo, copia la totalidad de los datos en otro juego de soportes, que puede consistir en servidores nube, storage y similares. La ventaja principal de la realización de un backup completo en cada operación es que se dispone de la totalidad de los datos en un único conjunto. Esto permite restaurar los datos en un tiempo mínimo, lo cual se mide en términos de tiempo de recuperación (RTO). No obstante, el inconveniente es que lleva más tiempo realizar un respaldo completo que de otros tipos (a veces se multiplica por un factor 10 o más), y requiere más espacio de almacenamiento ✓ Backups Tipo Incremental: Este tipo de Backup solo guarda la diferencia de datos entre la copia full inicial y la data generada posterior a la copia full. Una operación de respaldo incremental sólo copia los datos que han variado desde la última operación de backup de cualquier tipo. Se suele utilizar la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha de la última copia de seguridad. Las aplicaciones de respaldo identifican y registran la fecha y hora de realización de las operaciones de respaldo para identificar los archivos modificados desde esas operaciones, se puede ejecutar tantas veces como se desee, pues sólo guarda los cambios más recientes. La ventaja de un backup incremental es que copia una menor cantidad de datos que un respaldo completo. Por ello, esas operaciones se realizan más rápido y exigen menos espacio para almacenar la copia de seguridad. • Una vez realizada la tarea programada, las copias de seguridad se encontrarán almacenadas en los Data Storage (Discos duros de almacenamiento en la infraestructura del GORE Puno) referenciados por tipo de Backup y fecha de creación, dispuestos por la herramienta de generación de Backup. • Se cuenta con un esquema para realizar la revisión de restauración. Esta operación se debe realizar 1 vez al mes, sobre cada una Máquinas Virtuales de forma tal que se garantice que el backup quedó generado de forma correcta y su retención se hará de acuerdo a lo especificado por los lineamientos establecidos por gestión documental y las áreas involucradas. A continuación, se describen las actividades que se deben realizar para la restauración de las copias de respaldo: • Seleccionar el backup que se quiere restaurar, uno por cada servidor local. • Descomprimir el backup. • Restaurar el backup en un ambiente de Pruebas. • Comprobar el funcionamiento de la restauración y en caso de ser fallido actualizar el backup y el procedimiento del mismo, y probar nuevamente.
RESPONSABLE	Equipo de prevención
CONOCIMIENTOS	Aplicaciones y bases de datos
RECURSOS ESENCIALES	Sistemas de información, instructivos y equipos.

GOBIERNO REGIONAL OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN V° B° PUNO

FICHA 02: DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO SERVIDORES LOCALES (FISICOS)	
ACTIVIDADES ESENCIALES	• Realizar copias de respaldo de los servidores locales (físicos) que están en producción, de una manera óptima y práctica, para su posterior almacenamiento; por fechas, nombres y demás disposiciones para restauraciones programadas y de emergencia. • Es necesario realizar una copia de seguridad de los servidores locales en producción, que contenga la estructura en hardware y software, tales como Memoria, Procesamiento, Dispositivos de red, Discos duros virtuales, entre otros.
TIPO	Servidores Locales (Físico)
PROCEDIMIENTO	• Realizar las copias de seguridad backup cada un (01) día o máximo cada dos (02) días • Por medio de herramientas de copias de respaldo, se realiza la integración con la infraestructura Local correspondiente a los servidores físicos, y se seleccionan los que correspondan a producción, entre ellos servidor SIAF, SIGA, SIAL, similares: que correspondan al funcionamiento de la infraestructura tecnológica, entre otros que sean previamente solicitados. • Mediante la herramienta generadora de copias de respaldo, se realiza una programación de una tarea donde se ejecutarán periódicamente dos tipos de Backups: ✓ Backup Tipo Full: Este tipo de backup contendrá una copia íntegra del 100% del servidor local previamente seleccionado. Este tipo de respaldo, copia la totalidad de los datos en otro juego de soportes, que puede consistir en servidores de almacenamiento, storage y similares. La ventaja principal de la realización de un backup completo en cada operación es que se dispone de la totalidad de los datos en un único conjunto. Esto permite restaurar los datos en un tiempo mínimo, lo cual se mide en términos de tiempo de recuperación (RTO). No obstante, el inconveniente es que lleva más tiempo realizar un respaldo completo que de otros tipos (a veces se multiplica por un factor 10 o más), y requiere más espacio de almacenamiento ✓ Backups Tipo Incremental: Este tipo de Backup solo guarda la diferencia de datos entre la copia full inicial y la data generada posterior a la copia full. Una operación de respaldo incremental sólo copia los datos que han variado desde la última operación de backup de cualquier tipo. Se debe utilizar la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha de la última copia de seguridad. Las aplicaciones de respaldo identifican y registran la fecha y hora de realización de las operaciones de respaldo para identificar los archivos modificados desde esas operaciones, se puede ejecutar tantas veces como se desee, pues sólo guarda los cambios más recientes. La ventaja de un backup incremental es que copia una menor cantidad de datos que un respaldo completo. Por ello, esas operaciones se realizan más rápido y exigen menos espacio para almacenar la copia de seguridad. • Una vez realizada la tarea programada, las copias de seguridad se encontrarán almacenadas en los servidores de almacenamiento, Data Storage (Discos duros de almacenamiento en la infraestructura del GORE Puno) referenciados por tipo de Backup y fecha de creación, dispuestos por la herramienta de generación de Backup. • Se cuenta con un esquema para realizar la revisión de restauración. Esta operación se debe realizar 1 vez al mes, sobre cada una Máquinas Virtuales de forma tal que se garantice que el backup quedó generado de forma correcta y su retención se hará de acuerdo a lo especificado por los lineamientos establecidos por gestión documental y las áreas involucradas. A continuación, se describen las actividades que se deben realizar para la restauración de las copias de respaldo: • Seleccionar el backup que se quiere restaurar, uno por cada servidor local. • Descomprimir el backup. • Restaurar el backup en un ambiente de Pruebas. • Comprobar el funcionamiento de la restauración y en caso de ser fallido actualizar el backup y el procedimiento del mismo, y probar nuevamente.
RESPONSABLE	Equipo de prevención
CONOCIMIENTOS	Aplicaciones y bases de datos
RECURSOS ESENCIALES	Sistemas de información, instructivos y equipos.

GOBIERNO REGIONAL V° B° OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN PUNO

FICHA 03: DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE RESPALDO BASES DE DATOS	
ACTIVIDADES ESENCIALES	Realizar el proceso de backup de las bases de datos que se encuentran sobre la infraestructura *on premise* de la entidad para cada una de las aplicaciones teniendo en cuenta cada uno de los motores de base de datos.
TIPO	Bases de datos
PROCEDIMIENTO	• Realizar un dump de la base de datos. El dump de la base de datos debe depender del tipo de base de datos respectivo, por ejemplo: a. Mysql: mysqldump -u USER -p DB > "$archivo" && gzip "$archivo"; b. Postgresql: pg_dump -h IP -p PORT -U USER -d DB --format=custom > /DIR $nombre.backup c. Heidi SQL (interfaz gráfica): Export via > Tools > database Export • Una vez se realiza la copia se debe comprimir en un formato sql.gz o tar.gz. La verificación se debe hacer de dos formas: a. Fecha de modificación o creación: Para verificar si el backup se realizó en la fecha estipulada, se debe ubicar en la carpeta ($nombre_servidor). Al abrirla encontrará los archivos generados por la tarea programada en cada una de las unidades de almacenamiento externas, los cuales aparecen de la siguiente manera: b. Tamaño de Archivo: La verificación por tamaño de archivo se hará por cada una de las carpetas, en las unidades de almacenamiento externo de la siguiente manera: ✓ Backups DB: se abre la carpeta y se verifica el tamaño del archivo en la columna "tamaño" o "size" de la ventana. Ejemplo: Back_DB "size" 826,102 KB ✓ Backup_Diferencial: se abre la carpeta y se verifica el tamaño del archivo en la columna "tamaño" o "size" de la ventana. Ejemplo: Back_Diferencial "size" 262,156,980 KB. • Verificar el backup Para hacer el esquema de revisión de restauración. Esta operación se debe realizar 1 vez al mes, y sobre cada una de la base de datos de forma tal que se garantice que el backup quedó de forma correcta. a. Seleccionar el backup que se quiere restaurar, uno por cada base de datos b. Descomprimir el backup c. Restaurar el backup dependiendo de la base de datos: cd ..; cd /DIR/$nombre.sql | docker-compose exec -T db sh -c 'mysql -u USER -p CONTRASEÑA'
RESPONSABLE	Equipo de prevención
CONOCIMIENTOS	Aplicaciones y bases de datos
RECURSOS ESENCIALES	Sistemas de información, instructivos y equipos.

FICHA 04: DESCRIPCIÓN TÉCNICA PROCESO DE GENERACIÓN DE COPIAS DE CODIGO FUENTE APLICACIONES	
ACTIVIDADES ESENCIALES	Realizar la copia de seguridad sobre el código de las aplicaciones que son desplegadas en la infraestructura de la nube. El importante tener en cuenta que el código tiene un esquema redundante, por sí solo. Es decir, una copia existe en el repositorio de la entidad, una segunda copia en el servidor donde se despliega y una tercera copia con el desarrollador.
TIPO	Código fuente de las aplicaciones
PROCEDIMIENTO	La entidad debe contar con un repositorio en GIT en la nube. Todos los desarrollos Web deben estar en el repositorio de la entidad. Consideraciones: se debe contar con una cuenta en gitlab.com, github.com, git-scm.com, o alguna otra página de seguimiento de repositorio de versiones.
RESPONSABLE	Equipo de prevención
CONOCIMIENTOS	Aplicaciones y bases de datos
RECURSOS ESENCIALES	Sistemas de información, instructivos y equipos.