Trabajando para ti

Entidad Prestadora de Servicios de Saneamiento TACNA S.A.

RESOLUCION DE GERENCIA GENERAL Nº 502 -2021-300-EPS TACNA S.A.

TACNA, 24 DIC 2021

VISTO:

El Informe Nro. 169-2021-450-EPS TACNA S.A., Mediante el cual El JEFE DE LA OFICINA DE TECNOLOGIA DE LA INFORMACION hace llegar el Proyecto del Plan de Contingencia y Seguridad de la Información de la EPS TACNA S.A. para su aprobación.

CONSIDERANDO:

Que la ley Nº 28551, Ley que establece la obligación de elaborar y presentar Planes de contingencia, dispone que todas las personas naturales y jurídicas de derecho privado o publico que conducen y/o administran empresas, instalaciones, edificaciones y recintos tienen la obligación de elaborar y presentar, para su aprobación ante la autoridad competente, planes de contingencias para cada una de las operaciones que desarrolle.

Que la ley Nº 28716 "Ley de control interno de las Entidades del Estado", tiene por finalidad que las entidades del Estado incorporen obligatoriamente sistemas de control interno en sus procesos, actividades, recursos, operaciones y actos institucionales.

Que, con Informe de los vistos, la Oficina de Tecnología de la Información hace llegar el Proyecto del Plan de Contingencia y Seguridad de la Información de la EPS TACNA S.A. para el año 2021, por lo que luego de revisarlo es pertinente emitir Resolución;

Que, estando conferidas las facultades al Gerente General de dictar y emitir resoluciones y con VºBº de la Gerencia de Administración y Finanzas, Oficina de Asesoría Legal y la Oficina de Tecnología de la Información;

SE RESUELVE:

ARTÍCULO PRIMERO: Aprobar El Plan de Contingencia y Seguridad de la Información de la Entidad Prestadora de Servicios de Saneamiento Tacna S.A, el mismo que a folios (33) forma parte integrante de la presente Resolución.

ARTICULO SEGUNDO: Encargar a la Oficina de Tecnología de la Información el cumplimiento de la presente Resolución.

REGISTRESE Y COMUNIQUESE

ING. JUAN ALBERTO SEMINARIO MACHUCA
GERENTE GENERAL
EPS TACNA S.A.

Cc. GAF, OAL, OTI
Archivo

Av. Dos de Mayo N° 372 – Tacna
Telf. (052) 583446 – Fax (052) 583453
Mail: eps.informes@epstacna.com.pe

OFICINA DE
TECNOLOGIA DE LA INFORMACION

PLAN DE CONTINGENCIAS Y SEGURIDAD DE LA INFORMACION

Versión 2.0

2021

Av. Dos de Mayo N° 372 – Tacna
Telf. (052) 583446 – Fax (052) 583453
Mail: eps.informes@epstacna.com.pe

INTRODUCCIÓN

El presente plan de contingencias y recuperación elaborado para la entidad, responde a la necesidad de contar con un documento base para enfrentar problemas ocasionados por desastres naturales, incendios, inundaciones y alguna otra falla fortuita en los equipos de cómputo.

En la primera parte del documento se hace un inventario de los recursos informáticos con que cuenta la entidad, para luego diagnosticar los principales problemas que pueden sufrir estos equipos como consecuencia de algún incidente natural o fortuito. A partir de este diagnóstico se elabora el plan de acción preventivo y correctivo así como la formación de los equipos de trabajo para responder con prontitud ante estos hechos. Finalmente se detalla las actividades que cada responsable debe realizar durante y después de producida la emergencia.

Este manual debe ser permanentemente actualizado por las personas integrantes del equipo Administrador del Plan y los responsables de la Red de la Entidad, de tal forma que sea útil en el momento que se requiera.

PARTE 1: DEFINICIÓN DEL PROYECTO

1.1. Justificación del Proyecto

El objeto de este proyecto es establecer las normas, organización, responsabilidades y desarrollar procedimientos que permitan asegurar una eficiente capacidad de recuperación ante desastres y otras situaciones de emergencia en aspectos de informática, con el propósito de mantener la continuidad funcional del procesamiento de datos y de las aplicaciones vitales durante el tiempo que dure la recuperación, para ello se entregará a la Gerencia General de la entidad un manual de procedimientos operativos a utilizar cuando se produzca una contingencia.

Los (02) grandes ámbitos identificados en función de la magnitud de la contingencia son los siguientes:

- Se habla de desastre o catástrofe cuando lo sucedido implica la imposibilidad de continuar trabajando en el Centro de Proceso de Datos (entiéndase como Sala de Servidores), siendo imprescindible el traslado a un Centro de Proceso de Datos Alternativo, también llamado Centro de Backup o "Warm Site", cuyas características y niveles mínimos son también parte del estudio, así como los procedimientos de traslado, estancia en dicho Centro de Backup y retorno al Centro de Proceso de Datos original una vez desaparecidos los efectos de la contingencia.
- El otro gran ámbito es el de las llamadas contingencias "**in-house**", aquellas que no implican el traslado de las operaciones a un Centro de Procesamiento de Datos Alternativo pero que requieren también de la toma de medidas de tipo preventivo o correctivo por el impacto que producen en el nivel de servicio del Centro de Proceso de Datos y como consecuencia en la entidad.

El siguiente paso para el desarrollo del proyecto consiste en la determinación de equipos de trabajo. Designar responsables tanto del personal de cómputo, como de otras áreas involucradas en la seguridad de la información.

- **Un Equipo de Emergencia**. Realizará las tareas de recuperación y puesta en marcha del centro alternativo (Soporte Tecnológico y Administración de Redes).

- **Un Equipo de Mantenimiento del Plan**. Será el encargado de mantenerlo actualizado, realizando en él los cambios que resulten pertinentes, con motivo de cambios producidos en las personas o en los activos informáticos, o bien, con motivo de las experiencias obtenidas de la prueba o de la ejecución, en contingencia real del Plan (Responsable de Administración de redes).

- **Director del Plan**. Decidirá y dirigirá la puesta en marcha del plan.

- **Un Administrador del Plan**: Responsable del planeamiento y mantenimiento del plan.

Para la última etapa, será necesaria la elaboración de un Plan de Implantación ya que, en muchos casos, la puesta en marcha del Plan de Contingencias requiere de un período de transición en el cual realizar determinadas inversiones, completar cambios, los cuales serán especificados en el estudio.

Tener un plan de contingencias no siempre evita la catástrofe pero la minimiza. Existen ejemplos de muchas empresas que sufrieron un desastre y desaparecieron por no disponer de un Plan; en cambio otras empresas consiguieron resistir en circunstancias extremas por disponer de un Plan de Contingencias que les permitió actuar con rapidez al tener personal previsto y entrenado, mediante pruebas, tomando en conocimiento la forma de proceder ante la eventualidad de determinadas contingencias. Como sabemos no es fácil realizar una cuantificación en términos económicos de los recursos y los datos que se pierden cuando se produce una contingencia grave (desaparición de la entidad). Para disminuir estas pérdidas económicas debemos hacer todos los esfuerzos, protegiendo sus instalaciones, teniendo un centro de procesamiento alternativo que ayuden a soportar una contingencia grave y nuestra entidad tenga el menor tiempo posible sin operar minimizando las perdidas.

1.2. Generalidades

1.2.1. Reconocimiento del Entorno o Ambito

La EPS TACNA S.A., es una Empresa Municipal de derecho privado, constituida como Sociedad Anónima con autonomía administrativa, técnica y económica.

La EPS TACNA S.A. realiza todas las actividades vinculadas a la prestación de los servicios de agua potable, alcantarillado sanitario y pluvial y servicio de disposición sanitaria de excretas en el ámbito de su jurisdicción; éstas son de utilidad y necesidad pública de interés social.

La EPS TACNA S.A., tiene como ámbito de influencia las Provincias de Tacna y Jorge Basadre del Departamento de Tacna en la República del Perú.

La EPS TACNA cuenta con una Junta General de Accionistas,1 Directorio, 1 Gerencia General, 4 Gerencias de Líneas.

1.2.2. Visión

La EPS TACNA S.A. tiene como visión: "Ser una empresa competitiva de servicios de saneamiento líder en el País"

1.2.3. Misión

La EPS TACNA S.A. tiene como misión: "Brindar calidad en los servicios de saneamiento en forma eficiente y eficaz, estableciendo nuevos procesos de mejoramiento continuo para satisfacer a la población".

1.3. Finalidad

Al finalizar el proyecto, la Oficina de Tecnología de la Información dispondrá del Manual del Plan de Contingencias y Recuperación de la EPS TACNA, el cual tendrá incluido el Plan Operativo de Contingencias y Recuperación así como las recomendaciones y sugerencias respectivas.

1.4. Objetivos

Los objetivos para tener un plan de recuperación documentado, probado y listo para ser inmediatamente utilizado son:

1.4.1. Objetivos Generales

- Limitar las pérdidas financieras
- Minimizar la magnitud de la interrupción
- Definir políticas que minimicen el costo y tiempo de recuperación
- Definir servicios alternativos para complementar las aplicaciones críticas

1.4.2. Objetivos Específicos

- Recuperar la totalidad de capacidad de proceso luego de sucedida una contingencia.
- Mantener personal entrenado para manejar operaciones de recuperación y en condiciones de emergencia para satisfacer las exigencias que la labor demanda.

- Justificar los costos operativos que actualmente se deben mantener para realizar en trabajo de Soporte Técnico.

1.5. Alcances

El Plan de Contingencia y Recuperación resultante del presente proyecto, servirá para garantizar la continuidad funcional del procesamiento de datos dentro de la entidad y además podrá ser objeto base de publicación y difusión a toda la administración pública, instituciones usuarias, personal de la especialidad y afines.

1.6. Organización

La EPS TACNA S.A., para establecer un programa de contingencias y recuperación permanente en aspectos de informática deberá organizar lo siguiente:

- La ubicación del personal dentro del organigrama se mantendrá vigente.
- Designar al Director del Plan (Gerente General)
- Designar al Administrador del Plan (Jefe Oficina Tecnología de la Información)
- Conformación de un Equipo de Emergencia. Personal de soporte tecnológico y administración de redes.

Miembros	Cargo
Jose Luis Fuentes Cornejo	Especialista en Redes y Comunicaciones
Jackeline Pilco Romero	Especialista en Análisis y Programación
Martín Rosado Cisneros	Especialista en Análisis y Programación
Selman José Sanchez Vargas	Especialista en Sistemas Georreferenciados

1.7. Funciones y Responsabilidades

Durante el proceso de desarrollo, la realización de pruebas e implementación del plan, existe una serie de funciones y responsabilidades permanentes que recaen sobre los miembros que conforman los equipos.

Los miembros de los equipos serán responsables del funcionamiento y puesta en marcha del plan de contingencia y recuperación. También se encargarán de hacer las pruebas y simulación de contingencias.

1.7.1. Director del Plan

- Es una persona con la autoridad necesaria para declarar la contingencia ante los proveedores del servicio
- Único vocero autorizado para hacer declaraciones externas
- El Director del plan y (02) alternos deberán estar autorizados para solicitar el uso del servicio al centro de cómputo alterno cuando suceda la contingencia.
- El Director del Plan convocará a reunión de coordinación a los jefes de equipo para establecer las funciones que tendrán ante la Gerencia y las Divisiones usuarias de los sistemas.
- Gestionar los recursos necesarios ante la Gerencia General para la puesta en marcha de los equipos

1.7.2. Administrador del Plan

Las funciones permanentes del administrador del plan serán las siguientes:

Funciones del planeamiento previo al desastre

- Validar que el plan obedezca a los objetivos estratégicos de la empresa, asegurando que permita la recuperación de las funciones críticas en los tiempos adecuados
- Identificar los grupos que tendrán participación activa en la implementación del plan
- Revisar reportes del proyecto propuesto y procedimientos para los otros equipos
- Informar y educar al personal de la entidad acerca del plan
- Mantener la información actualizada
- Realizar las pruebas del plan

Funciones en el evento de un desastre

- Declarar que el plan de recuperación sea puesto en ejecución
- Instruir al líder del equipo de mantenimiento para que recuperen los documentos vitales para contingencia (manuales y procedimientos deben estar en lugar seguro)
- Determinar la disponibilidad de todos los empleados de la empresa
- Decidir la convocatoria de los líderes de equipo y miembros alternos en caso sea necesario
- Decidir sobre la ubicación del centro de control
- Poner una copia de todo el material en el centro de control
- Arreglos para gastos (pagos de facturas, etc.) en coordinación con División de Logística
- Mantener informado al Director del Plan.
- Coordinar las acciones con el equipo de emergencia y mantenimiento

1.7.3. Equipo de Mantenimiento de Plan de Contingencia y Recuperación

- Tener con alta disponibilidad la lista de proveedores actualizada
- Durante el desastre, ordenar los reemplazos ante proveedores de acuerdo a requerimientos actuales

- Debe actualizar los procedimientos de Copia de Seguridad y el Plan de Contingencia y Recuperación
- Planear y probar las alternativas de comunicación de los CPD (propio y alterno)
- Ejecutar las pruebas del plan

1.7.4. Equipo de Emergencia

- Restaurar las aplicaciones según las especificaciones y/o requerimientos
- Asegurarse que el procesamiento pueda llevarse a cabo tan pronto como las aplicaciones estén disponibles
- Asegurarse que la aplicaciones sean recuperadas sin errores y estén operativas
- Asegurar que el equipo de comunicaciones y las líneas de comunicaciones estén disponibles
- Realizar tareas de recuperación y/o de puesta en marcha de las aplicaciones en el centro de procesamiento alternativo.
-

1.8. Recursos

Los recursos que son necesarios para llevar a cabo la misión de resguardar.

1.8.1. Recursos Humanos

- Equipos conformados en el punto 1.6
- Personal de las Gerencias y Oficinas involucradas con las aplicaciones

1.8.2. Recursos materiales y apoyo complementario

- Oficina para establecer como centro de control durante una contingencia
- Equipo de cómputo preparado para trabajo de ofimática
- Impresora
- Pizarra acrílica
- Pizarra interactiva
- Proyector
- Plumones para pizarra acrílica
- Papel Bond-A4
- Suscripción a revista especializadas o material de Internet
- Información adicional que considere la administración del plan

1.9. Responsabilidades

Se ha determinado la necesidad de establecer los procedimientos que serán ejecutados por los equipos que han sido conformados:

- El Equipo de Mantenimiento de Plan de Contingencias, a fines de cada año calendario presentará la propuesta tecnológica para efectuar mejoras en la seguridad para el año siguiente, con el presupuesto correspondiente a fin de ser considerado dentro del presupuesto general de la EPS TACNA S.A.

- Iniciado el proyecto, se establecerá un cronograma de actividades de mantenimiento para los equipos, así como para el desarrollo de las simulaciones

de recuperación y se efectuará la difusión del plan de contingencia en las gerencias usuarias respectivas.

- El coordinador de equipo, preverá con antelación las herramientas que faciliten el desarrollo del proyecto así como los riesgos que deben ser salvados para garantizar la continuidad del proyecto durante su desarrollo e implementación.

- El coordinador de equipo, observará los métodos empleados en el Plan de Acción y Plan de Emergencia y elevará las propuestas de mejoras en los procedimientos al equipo administrador del plan, cada vez que lo considere necesario.

- El coordinador de mantenimiento deberá conocer exactamente donde se encuentra las aplicaciones críticas actualizadas que deben ser restauradas, para lo cual deben coordinar con el responsable del área de desarrollo.

PARTE 2: DETERMINACIÓN DE APLICACIONES CRÍTICAS E INVENTARIO DEL HARDWARE Y SOFTWARE BASE

2.1. Aplicaciones Criticas

Las aplicaciones críticas identificadas se presenta en el **cuadro N°.1**, estas aplicaciones están operando en los servidores hasta la fecha, periódicamente ingresan a producción nuevas aplicaciones y así mismo otras se retiran (backups históricos) por lo cual este cuadro debe ser actualizado en forma permanente por el responsable de producción.

El criterio empleado para clasificar el nivel de importancia y la prioridad del sistema utiliza una puntuación de: 1=Baja importancia, hasta 10=Alta importancia.

CUADRO NRO. 1: APLICACIONES CRITICAS PRODUCCIÓN

Aplicación	Servidor	Lenguaje	Puntaje	Procesamiento		Area Usuaria	
				Geren	Progra.	Gerencia	Usuario
SISTEMAS COMERCIAL:							
SIINCO	ARES	Windows 2008, PowerBuilder, Sybase	10	OTI	Jackeline Pilco Romero	GCOM	Todos usuarios comerciales
REPORTES SIINCO	ATENEA	Windows 7,Php, Mysql, Sybase	7	OTI	Jackeline Pilco Romero	GCOM	Todos usuarios comerciales
SIINCOWEB, SIINCOMOBIL	ATENEA	Ubuntu, Php, mysql	10	OTI	Jackeline Pilco Romero		CARS, Operadores de Medición

SISTEMA ADMINISTRATIVOS:							
AVALON (Sistema Integrado Administrativo)	SRVARCHIVOS	Visual FoxPro	10	OTI	Martín Rosado Cisneros	Todos	Todos
ASISTENCIA	EROS	Visual FoxPro	9	OTI	Martín Rosado Cisneros	GAF	RR.HH
SISTRAM (Tramite Documentario)	POSEIDON	Visual FoxPro	8	OTI	Martín Rosado Cisneros	Todos	Todos
SFIN (Inventario Informatico)	WEB INTRANET	Ubuntu, Php, Mysql	7	OTI	Jose Luis Fuentes	OTI	Todos
SISTEMAS ADMINISTRATIVOS ANTIGUOS	EROS	Visual FoxPro	5	OTI	Martín Rosado Cisneros	GAF	Todos
SISTEMA OPERACIONALES:							
SISOP (Sistema Operacional)	WIN-SO92QGJ7YEI	Windows 8, SQL Server	10	OTI	Martín Rosado Cisneros	GCOM, GOPE	Comercial, Operaciones
SISTEMAS COMPLEMENTARIOS:							
Portal Web	VIRTUAL MEDUSA	Ubuntu, Php, postgresql	10	OTI	Jose Luis Fuentes	Todos	Todos
Operaciones en Linea	SRVKARPESKY	Windows 2003, SQLSERVER2008, VS2010	10	OTI	Martín Rosado Cisneros	Todos	Todos
SICAP	EROS	Visual FoxPro	6	OTI	Martín Rosado Cisneros	Todos	Todos
SIAF	HERMES	Visual FoxPro	6	OTI	Martín Rosado Cisneros	GAF, GG	GAF, GG
OFICINA VIRTUAL	ATENEA	Ubuntu, Php, sybase	10	OTI	Jackeline Pilco Romero	Todos	Todos
PAGO VISA	VIRTUAL MEDUSA	Ubuntu, Php, postgresql	10	OTI	Jackeline Pilco Romero	Todos	Todos

SISTEMA GEOREFERENCIADO							
GIS	MEDUSA	Windows 12,R2 SQL Server 2012	10	OTI	Selman Sanchez Vargas	GCOM, GING	Comercial, Ingenieria
SISTEMA DE RECUPERACION DE DATOS							
Sistema Veeam Backup & Replications	CRONOS	Microsoft Windows Server 2016	10	OTI	Jose Luis Fuentes Cornejo	Todos	Todos

2.2. REQUERIMIENTOS PARA EL FUNCIONAMIENTO DE LAS APLICACIONES CRITICAS

Para cada una de las aplicaciones críticas se detalla los recursos para su funcionamiento y usuarios que tienen acceso. Los procedimientos de instalación y operación deben estar especificados en los respectivos manuales (sistema y usuario) de la aplicación.

2.2.1. Servidor: ARES (SERVIDOR)

- HP Proliant DL180 G6
- Procesador Xeon 2.4Ghz
- Memoria RAM 16Gb
- Particiones: 300Gb;300Gb;300Gb,300Gb
- SO: Microsoft Windows Server 2008 R2 Estandar Edicion SP1

2.2.1.1. Sistema de Integrado de Información Comercial (SIINCO)

- Recuperar la Base de Datos en SYBASE
- Recuperar un Instalador del Cliente Compilado
- Recuperar los Códigos Fuente.
- Para los Reportes SIINCO, pueden ser creados en el mismo servidor (antes realizados en el servidor EPS-2104)

2.2.2. Servidor: ARES (ATENEA)

- Servidor Virtualizado de un HP Proliant DL180 G6 con ESXI de VMWARE
- Sistema Operativo: UBUNTU SERVER 10.04.2 x64
- Procesador: Xeon 2.4Ghz
- Disco Duro 40 GB
- RAM: 1GB

2.2.2.1. Plataforma Web del SIINCO para CARS y Toma de Lecturas (SIINCOWEB)

- Verificar la Instalación de mySQL5.1.41, Apache2.2.0, Postgres, Samba, webmin1.550

- Recuperar las librerías de SYBASE para conectividad al servidor, junto con los sripts de conectividad
- Recuperar los Códigos Fuente (Script para el WWW).

2.2.3. Servidor: HERMES (SERVIDOR)

- HP Proliant DL360 G5
- Procesador Xeon E5310 1.6Ghz
- Memoria RAM 4Gb
- Particiones: 68Gb;68Gb
- SO: Microsoft Windows Server 2003 R2 Estandar Edicion SP2

2.2.3.1. Sistema Integrado Administracion y Fianzas AVALON

- Sistema SIAF
- Mapear la Unidad Compartida

2.2.4. Servidor: SRVARCHIVOS (SERVIDOR)

- HP Proliant DL360 G5
- Procesador Xeon 5310 1.6Ghz
- Memoria RAM 4Gb
- Particiones: 125Gb;125Gb
- SO: Microsoft Windows Server 2008 R2

2.2.4.1. Sistema Integrado Administrativo AVALON

- Recuperar Copia de Respaldo y Fuentes en el Servidor
- Recuperar Base de Datos Nativas de Visual FoxPro
- Recuperar Instalador del Cliente.
- Mapear la Unidad Compartida

2.2.5. Servidor: POSEIDON (SERVIDOR)

- HP Proliant ML370 G4
- Procesador Xeon 3.06Ghz
- Memoria RAM 4Gb
- Particiones: 136Gb;136Gb
- SO: Microsoft Windows Server 2003 R2 Estandar Edicion SP2

2.2.5.1. Tramite DocumentarioSISTRAM

- Recuperar Copia de Respaldo y Fuentes en el Servidor
- Recuperar Base de Datos Microsoft SQL SERVER 2005
- Recuperar Instalador del Cliente

2.2.6. Servidor: SRV-SISOP (SERVIDOR)

- Posibilidad de Ser usado en una Plataforma Virtualizada Esxi de VMWARE
- Procesador basado en Servidor
- Memoria RAM 4Gb
- Particiones: 136Gb;136Gb

- SO: Microsoft Windows Server 2008 R2

2.2.6.1. Sistema Integrado Operacional SISOP

- Recuperar Copia de Respaldo y Fuentes en el Servidor
- Recuperar Base de Datos Microsoft SQL SERVER 2008
- Recuperar instalador del cliente.

2.2.7. Servidor: EROS (SERVIDOR)

- HP Proliant DL380 G8
- Procesador Xeon 2.4Ghz
- Memoria RAM 24Gb
- Particiones: 100Gb;500Gb;400GB
- SO: Microsoft Windows Server 2008 R2 Estandar Edicion SP1

2.2.7.1. Sistema GEOreferenciado (Prueba)

- Recuperar Copia de Respaldo y Fuentes en el Servidor
- Recuperar Base de Datos Microsoft SQL SERVER 2008
- Instalar ARCGIS SERVER

2.2.7.2. Sistema de ASISTENCIA

- Base de datos y código fuentes del sistema de asistencia.
- Recuperar Copia de Respaldo y Fuentes en el Servidor
- Mapear la Unidad Compartida

2.2.7.3. Sistema Antiguos

- Base de datos y código fuente de los sistemas administrativos antiguos.
- Zona de Consulta.
- Mapear la Unidad Compartida de consultas.

2.2.8. Servidor: SRV-KARPESKY (SERVIDOR)

- Posibilidad de Ser usado en una Plataforma Virtualizada Esxi de VMWARE
- Procesador basado en Servidor
- Memoria RAM 4Gb
- Particiones: 136Gb;136Gb
- SO: Microsoft Windows Server 2008 R2

2.2.8.1. Plataforma de consultas en Linea de Recibos Facturados

- Recuperar Copia de Respaldo y Fuentes en el Servidor
- Recuperar Base de Datos Microsoft SQL SERVER 2008
- Recuperar instalador web IIS.

2.2.9. Servidor: MEDUSA (SERVIDOR)

- HP Proliant DL380 G10
- Procesador Intel Xeon 5118 2.30Ghz
- Memoria RAM 32Gb

- Disco Físico 1: 10 TB
- Disco Físico 2: 10 TB
- Disco Físico 3: 10 TB
- Disco Físico 4: 10 TB
- SO: Microsoft Windows Server 2012 R2

2.2.9.1. Sistema Georeferencial (GIS)

- Web Server GIS
- Base de Datos Microsoft SQL SERVER 2012
- Web Server Apache

2.2.10. Servidor: CRONOS (SERVIDOR)

- HP Proliant ML30 G9
- Procesador Intel Xeon E3-1220 3 Ghz
- Memoria RAM 8 Gb
- Disco Físico 1: 1 TB
- SO: Microsoft Windows Server 2016

2.2.10.1. Sistema VEEAM BACKUP & REPLICATIONS

- Sistema Veeam Backup & Replications

2.3. IDENTIFICACION DE COMPONENTES ESENCIALES Y CRITICOS

2.3.1. SOFTWARE

Son los elementos de software necesarios para asegurar la correcta ejecución de los sistemas o aplicativos de la institución:

SOFTWARE SERVIDOR	SOFTWARE CLIENTE
MS Windows 2003 Server R2	Windows 7
MS Windows 2008 Server R2, 2012, 2016	Visual Foxpro y Librerias
MS Exchange Server 2003 o Superior	Ms Office 2010
Sybase	Internet Explorer Ultima Version y Opera
ARCGIS Server	Visual Studio.Net
Microsoft SQL Server	ArcGis Desktop
Ubuntu Server 10 o 12 LTS	
ARCSoft Backup (recuperar backups)	
Esxi Vmware	Drivers de red e impresoras

Alta Prioridad

Acciones Preventivas

Los softwares de Alta Prioridad se han grabado una copia en CD y tambien se cuenta con una copia en EPS - Alto Lima Vigilancia.

2.3.2. EQUIPOS

2.3.2.1. Servidores

La institución actualmente cuenta con 20 servidores: 15 ubicados en la Oficina de Tecnología de la Información 2do piso (Centro de Datos), y 4 ubicados en el Centro de Datos de Alto Lima, 1 debajo de la oficina de operaciones los cuales se encuentran configurados y Operativos. Se debe de considerar para una recuperación de contingencia los equipos mencionados en los puntos **2.2.1** al **2.2.7**, para poder tener la continuidad de la plataforma.

2.3.2.2. Computadoras (PCs)

La Entidad cuenta con 153 PCs, de los cuales 99 están ubicadas en Dos de Mayo, 46 están en Planta Alto Lima y 08 están en la planta Calana. Para ejecutar las aplicaciones consideradas críticas, debemos contar mínimo con 20 PCs. Las características técnicas de estos equipos varían siendo estos como mínimo: PC Intel I3 o I5 de 2.6 GHZ o superior, 4096 MB de RAM y 500GB de espacio libre en disco. Estos equipos tienen el Sistema Operativo Windows 7 de preferencia a 64 bit.

2.3.2.3. Impresoras

En caso de emergencia la impresora necesaria para operar son

- 01 Laser HP Laser Jet M609 (para impresión de recibos),
- 01 Fotocopiadora Kyocera KM-2050 o superior; y
- 05 impresora matricial y 02 impresoras a tonner para la parte administrativa.

2.3.3. Equipos de Comunicaciones

En la Sede de 2 de Mayo

- Cableado Estructurado a Cat 6 Certificado que permite hasta 1 Gb, de acuerdo a normas y estándares nacionales e internacionales.
- Router Cisco 1800 Series
- FortiGate 200D
- Alcatel - OmniSwitch 6850-24
- Alcatel - OmniStack LS 6248
- Alcatel - OmniStack LS 6248
- Radio Enlace Ubiquiti NanoStation M5
- Radio Enlace Canopy Master (Para voz)

En la Sede Planta Alto de Lima

- Radio Enlace Master Alto Lima – 2 Mayo Ubiquiti NanoStation M5
- Radio Enlace Slave Alto Lima - Calana Ubiquiti NanoStation M5
- Radio Enlace Canopy Slave (Para voz)
- Alcatel - OmniStack LS 6224 (Almacén Central)

En la Sede Planta Alto de Lima

- Swicth Gigabit TrendNet 24 Puertos
- Radio Enlace Master Calana Ubiquiti NanoStation M5

ACCIONES PREVENTIVAS

Realizar los mantenimientos preventivos durante el periodo de garantía a los diferentes equipos, y luego negociar una extensión de mantenimiento preventivo y correctivo de ser el caso.

2.3.3.2. ROUTER PROVEEDOR CLARO (Acceso Internet).

Situación : Operativo. Permite la conexión a Internet y Correo Electrónico Externo, además permite el acceso desde el exterior a la publicación de la Pagina Web de la Empresa, debido a la configuración de un pool de IP públicas.

ACCIONES PREVENTIVAS

Firmar un contrato con una empresa proveedora de estos equipos con el propósito de obtener un reemplazo inmediato por otro equipo de similares características o uno superior compatible con la tecnología y los estándares de comunicación internos.
Se recomienda contar con alta disponibilidad se contrate los servicios de un segundo operador de internet con menores características y costos para poder dar continuidad a las operaciones de la entidad.

2.3.4. Equipos Electricos

Sub-Estación: Se encuentra ubicada en el primer piso, recibe el fluido eléctrico trifásico externo y distribuye la alimentación por pisos con llaves termostáticas. Cabe mencionar que es completamente independiente del fluido eléctrico para el alumbrado del edificio con la conexión para equipos informáticos.

2.3.4.1.UPS Paralelo Redundante con Tecnología True on Line: Se cuenta actualmente con 2 UPS y su respectivo transformador de aislamiento distribuidos de la siguiente manera: Centro de Datos Dos de Mayo y Centro de Datos Alto Lima, los mismos que están inoperativos, se recomienda se adquieran nuevos UPS.

2.3.4.2.Pozo de Tierra: Se cuenta actualmente con 12 pozos a tierra, nos provee la funcionalidad de absorber y/o derivar cualquier exceso o pico de tensión del sistema de energía eléctrica. Siendo la distribución la siguiente:

Sede 2 de Mayo
Un arreglo delta de 3 pozos para datos, ubicado en el patio.

Sede Alto de Lima
Dos pozos frente al edificio de Ingeniería para datos.

Un pozo al costado de la torre, para la solución de radio enlace y torre.
Tres pozos al costado de Almacén para datos

Sede Calana
Dos pozos al costado del edificio para datos
Un arreglo delta de 3 pozos frente a la torre para la solución de radio enlace.

ACCIONES PREVENTIVAS

- Confeccionar procedimientos de apagado y encendido del UPS en condiciones normales y en condiciones de emergencia
- Las personas que ingresen a los ambientes del UPS y de la Sub Estación deberán contar con la correspondiente autorización.

OBSERVACIONES

- De producirse un incendio y se corte la energía eléctrica, también nos quedaremos sin agua, lo cual sería contraproducente para poder apagar el incendio
- De producirse una inundación apagar de inmediato la sub-estación, el estabilizador y el UPS, pero debe observarse que el banco de baterias del UPS también tiene energía y deberá esperarse que se pierda la carga antes de efectuar alguna operación con el equipo, luego de inundado el ambiente.

2.4 AMBIENTE DE LOS EQUIPOS QUE SOPORTAN LAS APLICACIONES CRITICAS

Los Equipos (servidores) que soportan nuestra información se encuentran ubicados en la Oficina de Informática (2do piso), a este ambiente se le conoce como Sala de Servidores o Data Center. En la sala de servidores identificamos tres tipos de problemas que ponen en peligro la seguridad de la información:

2.4.1.Equipos de Aire Acondicionado.

Específicamente la sala de servidores cuenta con 1 equipo de aire acondicionado. Estos se encuentran operando con normalidad, se ha previsto la compra de uno de 36000 BTU de precisión.

2.4.2.Acceso a la Sala de Servidores.

Actualmente el acceso a la sala de servidores no está completamente restringida, no cuenta con un mecanismo automatizado que permita el ingreso solo al personal de soporte técnico, para ello se están realizando los trabajos para brindar una verdadera seguridad al Data Center:

PARTE 3: PLAN DE ACCIÓN PARA ESTRATEGIAS DE RECUPERACIÓN Y PREVENCIÓN DEL DESASTRE

El siguiente Plan de Acción para la Seguridad de la Información de la Red Institucional tiene por objetivo:

- Normar el proceso de realizar copias de seguridad periódicas de los servidores y de los discos duros de estaciones

- Evitar pérdidas de datos o posibles daños provocados por fallos en el disco duro, interrupción de la corriente eléctrica, infección por virus y muchos otros posibles problemas comunes en una red de equipos de cómputo.

3.1 Ubicación de las copias de respaldo

La intención es tener una lista de lugares de almacenamiento de las copias de respaldo a los cuales podremos acudir sucedida una contingencia y tener la necesidad de poner operativo el plan de recuperación de la información. Es preciso mencionar que estas instalaciones cuentan con un ambiente refrigerado y aislado debido a que las copias de respaldo son susceptibles al deterioro orgánico si no se encuentran en un ambiente frío, sin humedad y libre de campos magnéticos.

3.1.1 Locales de Almacenamiento Externo: Lugar donde se custodiará un juego de las copias de las aplicaciones críticas, configuración de servidores y software original:

- EPS TACNA S.A. – Caja Fuerte ubicada en Sala Eléctrica
  Dirección: Dos de Mayo Nº 372
  Telf.: 583446 – 1158 ó 1113
  Contacto: Jackeline Pilco R, Jose Luis Fuentes
- PLANTA ALTO LIMA – Estante ubicada en Centro de Datos
  Dirección: Alto Lima
  Telf.: 583446 – 2202, 1158 ó 1113
  Contacto: Jose Luis Fuentes, Jackeline Pilco R

3.1.2 Locales de almacenamiento Interno: Lugar donde se guarda el juego de las copias de respaldo generadas y primera fuente de recuperación luego de ocurrida una contingencia:

- OTI – Oficina de Tecnología de la Información
  Dirección: Dos de Mayo Nº 372
  Telf.: 583446 - 1113
  Contacto: Jose Luis Fuentes Cornejo
  Bóveda: Caja Fuerte ubicada en Sala de Eléctrica

3.2. Plan de copias de respaldo.

El plan de copias de respaldo se realiza por Servidor. El Administrador de la Red es el encargado de realizar las Copias de Respaldo correspondientes y hacer las actualizaciones tanto en el local interno como externo. Concluido el proyecto y respaldo la información se debe coordinar para eliminar los directorios de trabajo del servidor.

Respecto a las copias de respaldo del Software Original y la Configuración del Software Base Instalado, este incluye el respaldo de las particiones de arranque de los servidores.
Los medios que se emplearán para hacer los respaldos de la información son CDs, DVDs, BR y DD externos, cintas magneticas.

Cada uno debe estar identificado con una etiqueta:
Una etiqueta de cinta deberá de contener lo siguiente:

- Identificación del Medio
- Información completa acerca del contenido de la cinta (máquina, directorio, aplicación, directorio de red, etc.)
- Fecha de copia
- Fecha de verificación de copia

3.2.1 Ciclo de Rotación del Respaldo

Se encuentra Detallado en el plan de Backup que se adjunta al presente documento.

3.3. Estrategia de Recuperación.

Luego de sucedida una contingencia, dependiendo del nivel de desastre ocasionado se puede plantear dos estrategias de recuperación:

- Contingencia baja (Solución "in-house"): No plantea necesidad de trasladar las operaciones fuera de los ambientes de la Entidad, pero si implica realizar labores correctivas para regresar las operaciones a un estado de normalidad

- Contingencia alta (Solución "Warm Site"): Definida como desastre, trae como consecuencia la imposibilidad física de continuar trabajando en el Centro de Proceso de Datos propio (entiéndase como sala de servidores), y plantea la necesidad de trasladar las operaciones a un Centro de Proceso de Datos Alternativo. Para ello, se especificarán los pasos que se deben realizar para el traslado y mantener las aplicaciones críticas operativas hasta que sea posible el retorno al Centro de Proceso de Datos original

Para ambos niveles de desastre, es imprescindible contar con copias de respaldo de las aplicaciones, base de datos, software base y configuraciones de los servidores para una efectiva estrategia de recuperación.

Observaciones:

- Sucedida una contingencia, en primer término se deberá recurrir a las copias de respaldo ubicadas en los locales de almacenamiento interno.

- Si estos locales también han sido siniestrados, se procederá a declarar la contingencia ante los locales de almacenamiento externo para retirar las correspondientes copias de respaldo.

3.4 Informe técnico de configuración de equipos (Hardware – Software) para Backup

Hardware

El tipo de medio disponible y actualmente utilizada para las copias de seguridad de servidores son:

- (02) Quemadoras Externa de Blue Ray/ DVD / CD. CINTAS MAGNETICAS Con los que se puede extraer las copias de respaldo de los distintos medios.

Software

- (01) servidor con el Software VEEAM BACKUP & REPLICATIONS como sistema de copia de respaldo en cinta

3.5 Equipos responsables de recuperación

El equipo desde el punto de vista preventivo y correctivo, que debe hacer frente a una contingencia es:

- Equipo de Mantenimiento de Plan de Contingencias y Recuperación

La Oficina de Tecnología de la Información cuenta con 01 servidor que tiene la Quemadora Externa de Blue Ray/ DVD / CD / CINTAS MAGNETICAS.

PROCEDIMIENTO

El procedimiento de Backup (Copias de Seguridad) se encuentra detallado en Plan de Backup.

Trabajando para ti

EPS

Entidad Prestadora de Servicios de Saneamiento
TACNA S.A.

PLAN DE BACKUP

TACNA - PERU
2021

PLAN DE BACKUP Y RESPALDO

Eps Tacna S.A. cuenta con un procedimiento diario de Copias de Seguridad de los Sistemas Informáticos y consta de los siguientes términos:

1. OBJETIVOS

1.1. Garantizar la Integridad de la Información contenida en Cintas Magnéticas como medida preventiva a una contingencia en el Sistema de Información EPS Tacna S.A.

1.2. Reguardar las Copias de Seguridad con Información de los Servidores de la Sede Principal.

2. LUGAR DE CUSTODIA

Se trasportará el Backup (Cintas Magnéticas) en un compartimiento seguro y hermético para evitar el deterioro.

El lugar de custodia principal está ubicado en una caja fuerte en vigilancia en la Sede Principal.

La Caja Fuerte es en un lugar seguro y bajo llave, donde se resguarda la copia de Seguridad Mensual, libre de potenciales contingencias.

3. EXPOSICIÓN A LOS RIESGOS

De ocurrir alguna contingencia (pérdida, robo, deterioro) durante el tránsito de las cintas magnéticas, no tendría mayor impacto salvo el costo del mismo.

Sin embargo, lo acontecido anteriormente requiere la evaluación respectiva, a fin de determinar si amerita la denuncia policial correspondiente y la difusión en medios periodísticos para recuperar la cinta.

La información contenida tiene valor solo para la empresa y de querer ser mal utilizada en beneficio de terceros, no será posible puesto que requiere de una Clave de Acceso para la lectura de la información contenida. Esta Clave de Acceso solo es de conocimiento del Jefe de la Oficina de Tecnología de la Información y del Administrador de Rede y Comunicaciones.

4. PLAN ACTUAL

En este el plan de contingencia se está utilizando Cintas Magnéticas con una capacidad de 5.5 TB.

4.1. Plan de Copias de Respaldo

El plan de copias de respaldo se realizan por Servidor. El Administrador de la Red es el encargado de realizar los backups correspondientes y hacer las actualizaciones tanto en el local interno como externo.
Concluido el proyecto y respaldo la información se debe coordinar para eliminar los directorios de trabajo del servidor.
Respecto a las copias de respaldo del Software Original y la Configuración del Software Base Instalado, Base de Datos, donde podemos incluir el respaldo de las particiones de arranque de los servidores.

Los medios magnéticos que se emplearán para hacer los respaldos de la información son cintas magnéticas de 5.5 TB. Cada uno debe estar identificado con una etiqueta:

La cinta Magnetica deberá de contener lo siguiente:

- Identificación de la Cinta
- Información completa acerca del contenido de la Cinta (máquina, directorio, aplicación, directorio de red, etc.)
- Fecha de copia
- Fecha de verificación de copia

4.1.1. Ciclo de Rotación de la Cinta Magnética

El esquema del ciclo de rotación de **cinta magnética** es como sigue:

4.1.1.1. Modelo de rotación de cinta magnética para aplicaciones y SMBDR

- Una copia al disco duro Interno diario
- 1 Cinta magnetica mensual
- 1 Cinta magnetica anual

Modelo de Rotación de Cinta

Abril 2018						
D	L	M	M	J	V	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

	Backup Diario		
	Backup Mensual		

En el gráfico se muestra el esquema de rotación de cinta magnética para el mes de abril de 2018, del cual podemos detallar lo siguiente:

- (Dia 30) Se efectuará el proceso de copia de respaldo mensual
- De lunes a viernes se efectuarán los procesos correspondientes a una copia de respaldo diario. Estas copias seran duplicadas para enviar a los centros de respaldo alternativo.

Copia de Seguridad Normal: Diariamente de Lunes a Viernes se hacen copias de seguridad en en disco Duro Externo; a las 22:00. Esta técnica ofrece la posibilidad de restaurar tanto las aplicaciones como las Base de Datos de los diferentes Sistemas Administrativos y Comerciales.

Ventaja

- Los archivos son fáciles de encontrar puesto que siempre están en una copia de seguridad actual de su sistema o en un solo Disco Blue Ray.

Desventaja

- En caso de contingencia alta, puede haber perdida definitiva de este backup debido a que es guardado internamente .

Observaciones:

- Sucedida una contingencia, en primer término se deberá recurrir a la copias de respaldo ubicadas en los locales de almacenamiento interno.

- Si estos locales también han sido siniestrados, se procederá a declarar la contingencia ante los locales de almacenamiento externo para retirar las correspondientes copias de respaldo .

5. PROCEDIMIENTO PARA RECUPERACIÓN DE BACKUP

El procedimiento indicado se efectuará sobre un conjunto de Cinntas magneticas Backup, las mismas que estarán etiquetadas adecuadamente para su fácil identificación y respetando una secuencia cronológica y cíclica, de tal manera que disponemos de las copias de respaldo de los últimos 10 días hábiles con información recientemente actualizada de las Aplicaciones y SMBDR de la EPS Tacna S.A.

Para tal propósito indicamos que:

5.1. Diariamente, la Copia de Seguridad se obtiene de los Servidores de la **Sede Principal.**

5.2. En horas de la noche a partir de las 22:00 Horas, se inicia el proceso de Copia de Seguridad de los siguientes Servidores SISOP (Sistemas SISOP), Servidor GIS (Sistemas GeoReferenciado GIS - SICAT), Servidor PANDA (Tramite Doc), Servidor Calana (Sistemas Reclamos Operacional y complementario), Servidor ARES (Sistema Comercial), además del Servidor SRVArchivos donde se ubica los Sistemas administrativos (Avalon), también el Servidor Eros (Sistemas

Administrativos Antiguos) ubicado en la Sala de Servidores de la Oficina de Tecnología de la Información en la Sede Principal.

5.3. Todos los días de lunes a viernes, a primera hora de la jornada, los archivos que conforman la copia de respaldo del **Veeam Backup & Replication** se resguardan en los ambientes de la Oficina de Tecnología de la Información, haciendo el respectivo registro digital con los datos de Identificación de cada proceso.

5.4. La Cinta magnética Backup generada del **Veeam Backup & Replication** el último día hábil del mes, corresponde al Backup Mensual, y se resguarda en un ambiente fuera de la Oficina de Tecnología de la Información, el cual se ubica en una Caja Fuerte.

APLICACIONES QUE SE RESPALDAN

Las aplicaciones que se hacen backup se indican en el siguiente cuadro.

Aplicación	Servidor	Lenguaje	Contenido
SISTEMAS COMERCIAL:			
SIINCO	ARES	Windows 2008, PowerBuilder, Sybase	Aplicaciones y BD
SIINCO	ARES	Windows 2008, PowerBuilder, Sybase	Procesos Ciclo de Facturación
REPORTES SIINCO	ATENEA	Ubuntu, Php, mysql	Aplicaciones y BD
SIINCOWEB, SIINCOMOBIL	ATENEA	Ubuntu, Php, mysql	Aplicaciones y BD
SISTEMA ADMINISTRATIVOS:			
AVALON (Sistema Integrado Administrativo)	HERMES	Visual FoxPro	Aplicaciones y BD
ASISTENCIA	MARTE	Visual FoxPro	Aplicaciones y BD
SISTRAM (Tramite Documentario)	PANDA	Windows 8, SQL Server	Aplicaciones y BD
SISTEMA OPERACIONALES:			

SISOP (Sistema Operacional) Modulo Distribucion Modulo Mantenimiento Modulo Seguridad Modulo Ingenieria BioStar EPSTareos	SISOP	Windows 8, SQL Server	Aplicaciones y BD
SISTEMA RECLAMOS OPERACIONAL Y COMPLEMENTARIO:			
Modulo Operacional	Servidor Calana	Windows 8, SQL Server	Aplicaciones y BD
SISTEMAS COMPLEMENTARIOS:			
GIS	Servidor MEDUSA GIS	Windows 2012, SQL Server	Aplicaciones y BD
Portal Web	WEBEPS	Ubuntu,Php, Posgree	Aplicaciones y BD
Operaciones en Linea	SRVKARPESKY	Windows 2003, SQLSERVER2008, VS2010	Aplicaciones y BD
SISTEMA DE RESPALDOS:			
Servidor Backup	CRONOS	Windows 2016,	Aplicaciones y BD

Los backups se hacen desde el servidor CRONOS que cuenta con la unidad Backup (F). La programación de los backups automáticos se realizan con el VEEAM Backup & Replication 9.5

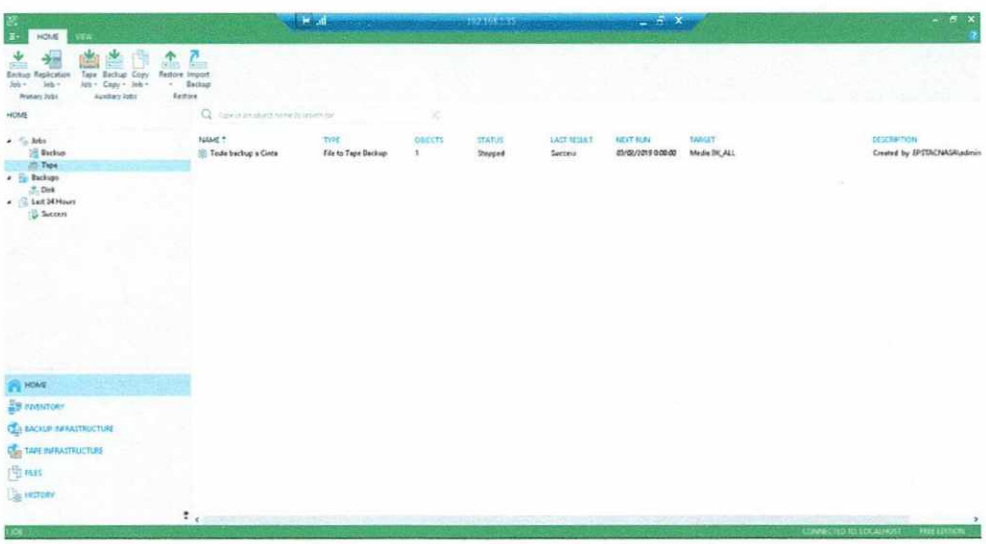
Para finalmente llevarlos a cintas magnéticas.

6. PROCEDIMIENTO PARA OPERACIÓN BACKUP DEL SOFTWARE VEEAM BACKUP & REPLICATION

El presente documento es un manual de recuperación de nuestros archivos respaldados (de ahora en adelante BACKUPS) mediante el Software VEEAM BACKUP & REPLICATION, y el cual tiene una programación de BACKUPS la cual se realiza en los mismos discos duros del servidor, específicamente en la Unidad E:\ del Servidor con capacidad de 1 TERABYTE.

El Servidor de Respaldos tiene las siguientes características:

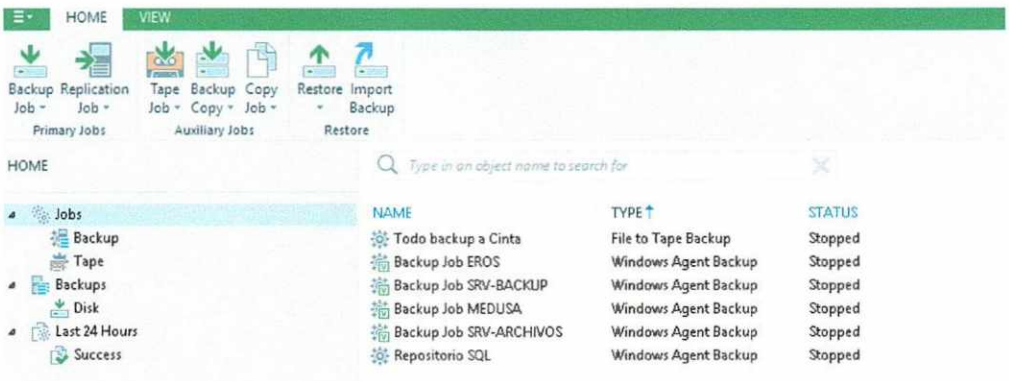
- Computadora HP Proliant ML30 Gen9, Procesador E3-1220 de 3.00Ghz, con 8 GB de RAM, Disco Duro para el Sistema de 1 Tb (Partición de 500GB y 500GB), y otro Disco Duro de 3TB para contenedor de los BACKUPS.
- Sistema Operativo Microsoft Windows 2016 Standard, registrado en el Dominio y de nombre de equipo CRONOS
- Software de Respaldo VEEAM BACKUP & REPLICATION



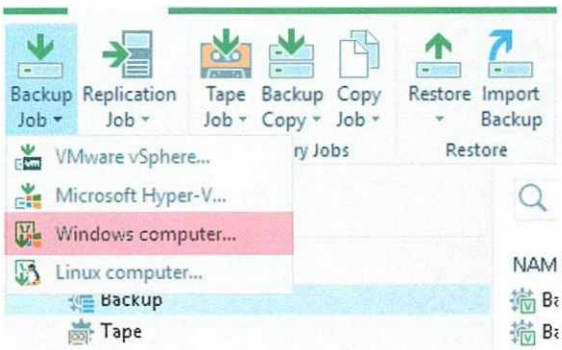
- Tener en cuenta que las 6 licencias que se posee son de los agentes del VEEAM BACKUP que se instalan en servidores clientes. Y el servidor backup es el básico de licencia gratuita.

1. CREACIÓN DE TRABAJOS (JOBS)

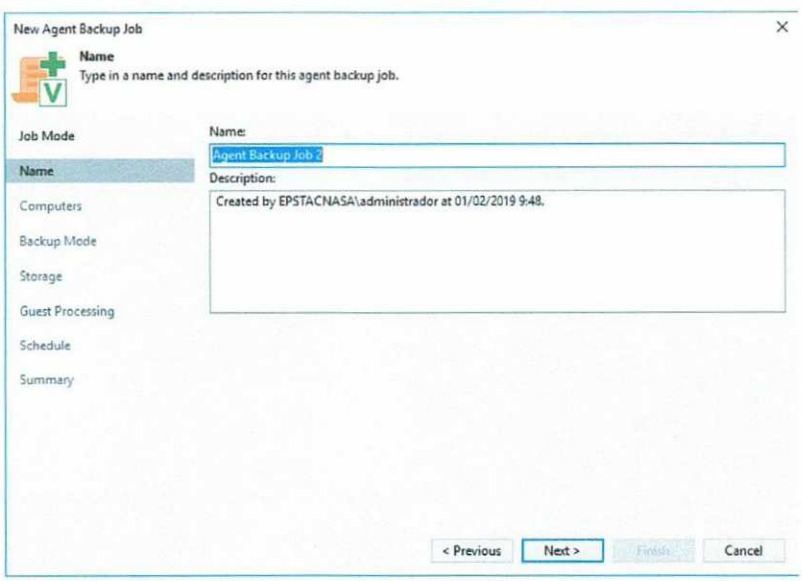
El trabajo es el procedimiento para realizar una copia de archivos de alguna ruta específica ya sea en el mismo servidor o en algún servidor cliente.

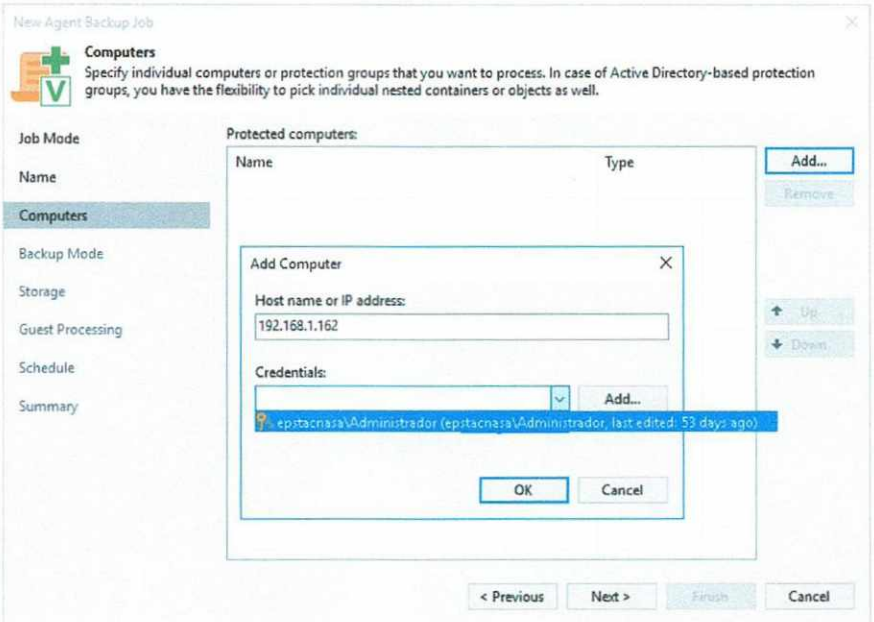


En la opción de Backup Job seleccionaremos Windows computer, debido a que los servidores de la empresa tienen la característica de poseer el sistema operativo Windows.

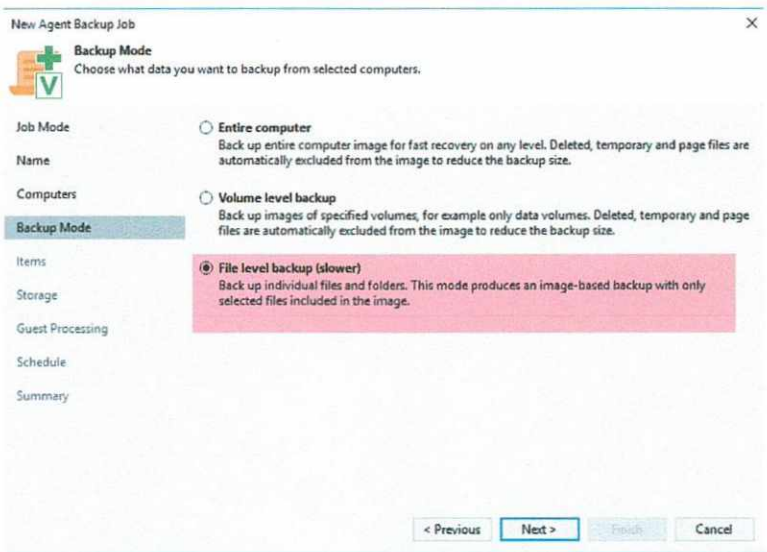


El trabajo se puede programar desde el cliente o el servidor CRONOS

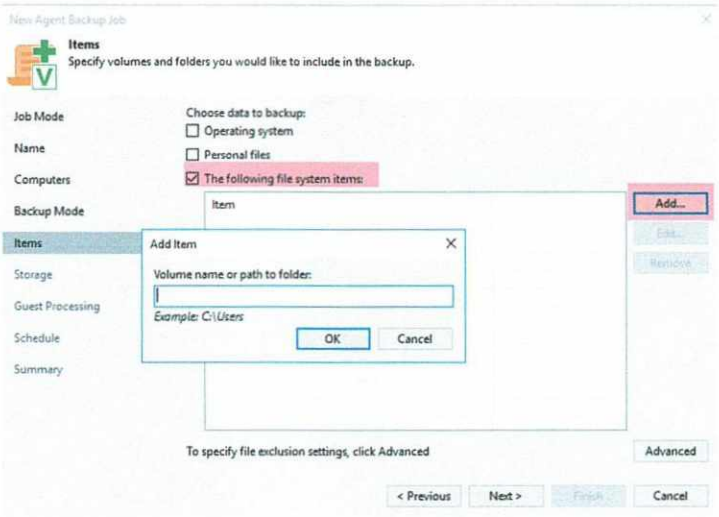




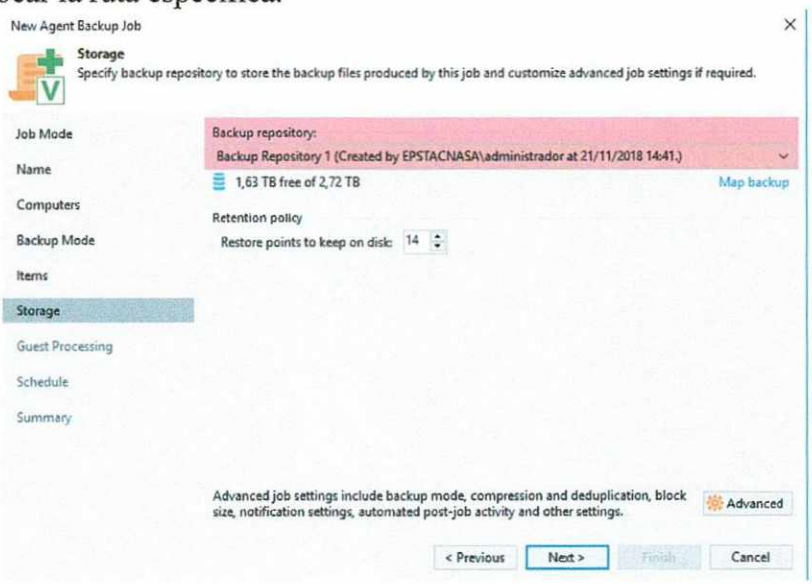
Se debera colocar el nombre del trabajo, y en la opcion Add agregar la direccion IP o Hostname en donde se encuentran los archivos a backapear, luego elegir o agregar las credenciales que cuenten con los permisos para realizar el trabajo.



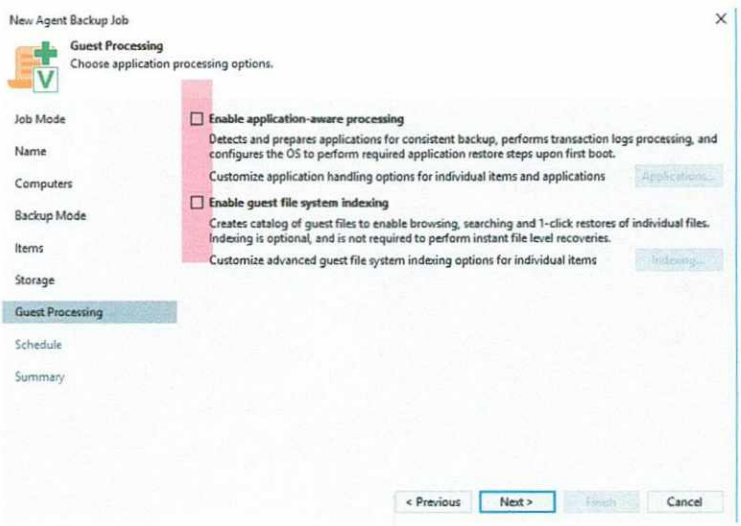
En el modo de backup te permite realizar 3 modos, mayormente se realizara el "File level Backup" que permite backapear especificos archivos de alguna unidad.



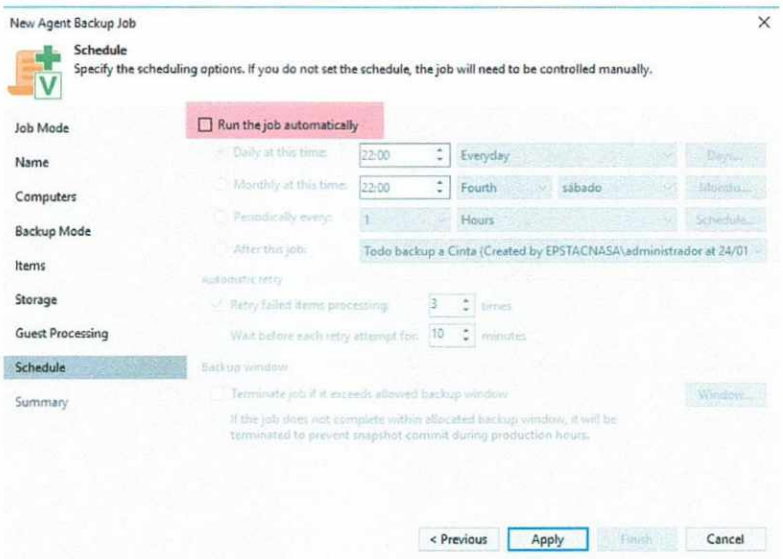
A continuacion en la ventana de "Items" se debe elegir la tercera opcion y en Add, colocar la ruta especifica.



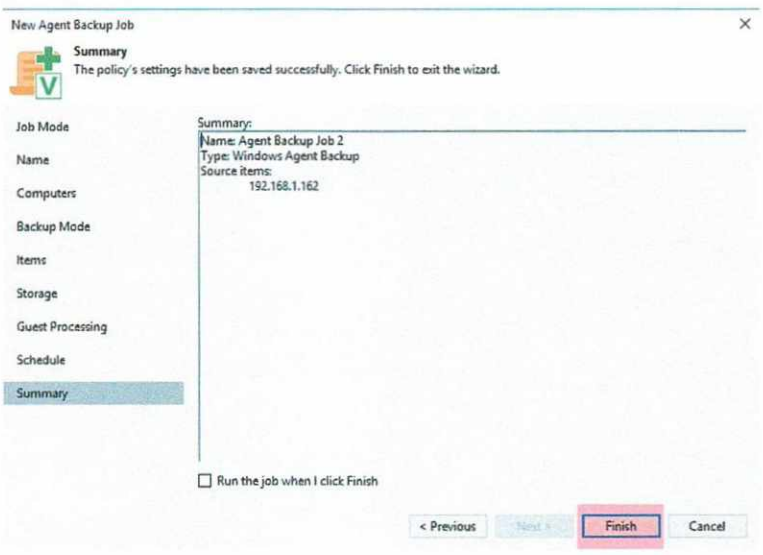
En la ventana "Storage" selecionara por defecto el unico repositorio que se encuentra en el servidor CRONOS.



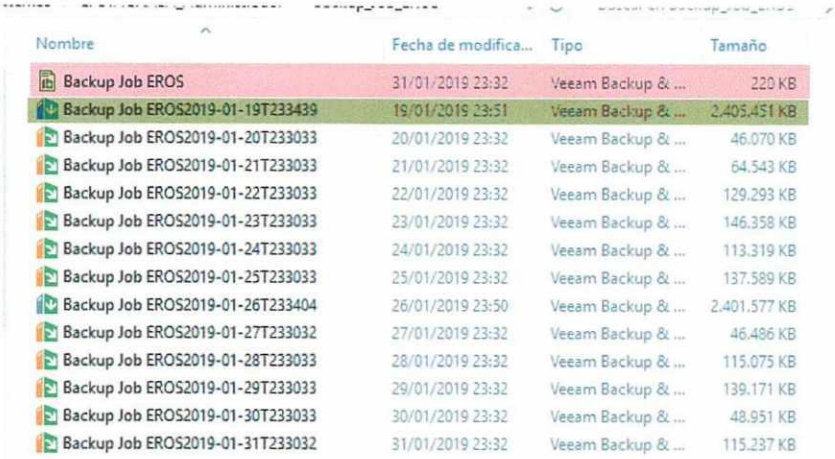
En la ventana Guest Processing, se presentaran opciones avanzadas, para realizar copias ya sean para realizar copias de toda la computadora o de archivos especificos, se puede omitir el paso sin perjuico del proceso.



En "Schedule" se programa la tarea para que se ejecute diaiamente o en algun evento especifico, si se desahibilta puede creara la tarea, pero debera ser ejecutada manualmente.



En la siguiente ventana se mostrara el resumen del trabajo y con eso se finaliza.



Nombre	Fecha de modifica...	Tipo	Tamaño
Backup Job EROS	31/01/2019 23:32	Veeam Backup & ...	220 KB
Backup Job EROS2019-01-19T233439	19/01/2019 23:51	Veeam Backup & ...	2.405.451 KB
Backup Job EROS2019-01-20T233033	20/01/2019 23:32	Veeam Backup & ...	46.070 KB
Backup Job EROS2019-01-21T233033	21/01/2019 23:32	Veeam Backup & ...	64.543 KB
Backup Job EROS2019-01-22T233033	22/01/2019 23:32	Veeam Backup & ...	129.293 KB
Backup Job EROS2019-01-23T233033	23/01/2019 23:32	Veeam Backup & ...	146.358 KB
Backup Job EROS2019-01-24T233033	24/01/2019 23:32	Veeam Backup & ...	113.319 KB
Backup Job EROS2019-01-25T233033	25/01/2019 23:32	Veeam Backup & ...	137.589 KB
Backup Job EROS2019-01-26T233404	26/01/2019 23:50	Veeam Backup & ...	2.401.577 KB
Backup Job EROS2019-01-27T233032	27/01/2019 23:32	Veeam Backup & ...	46.486 KB
Backup Job EROS2019-01-28T233033	28/01/2019 23:32	Veeam Backup & ...	115.075 KB
Backup Job EROS2019-01-29T233033	29/01/2019 23:32	Veeam Backup & ...	139.171 KB
Backup Job EROS2019-01-30T233033	30/01/2019 23:32	Veeam Backup & ...	48.951 KB
Backup Job EROS2019-01-31T233032	31/01/2019 23:32	Veeam Backup & ...	115.237 KB

En el repositorio puede crear hasta 3 tipos de archivos:

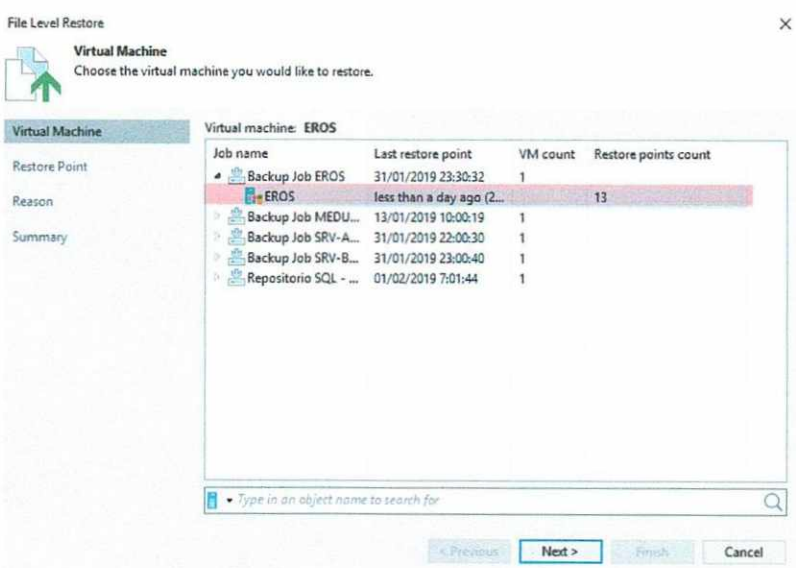
- La cabecera, que es la estructura del trabajo.
- El Full backup
- El Incremental Backup

Considerar estos archivos para la restauracion de algun backup.

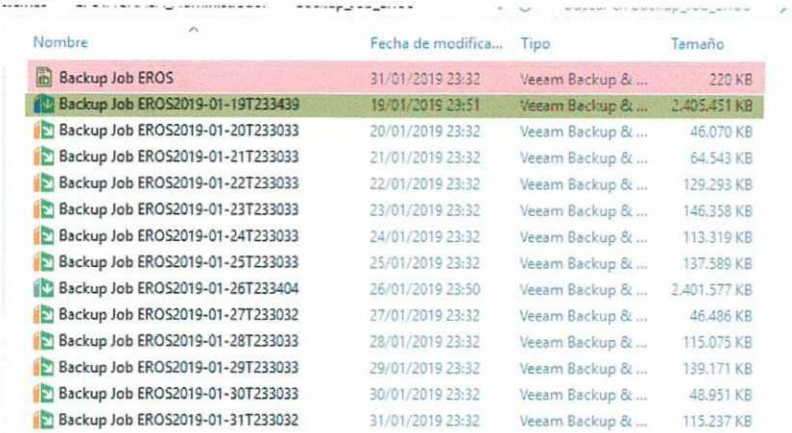
2. PROCEDIMIENTO PARA LA RECUPERACIÓN DE UN RESPALDO

Si se desea recuperar alguna copia de respaldo realizada se seleccionara la siguiente opción:

Al seleccionar aparecer la lista de los trabajos actuales para elegir

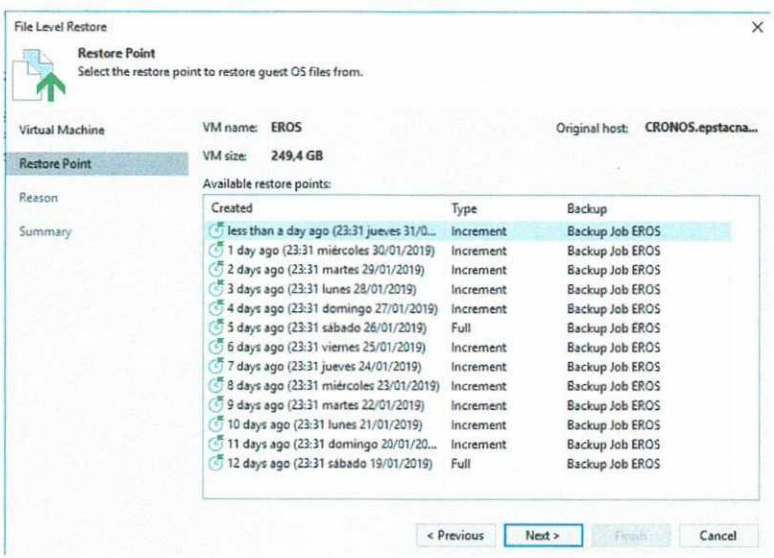


En caso de que no se encuentre el trabajo que se desea, seleccionar en el repositorio, o en la carpeta en donde se encuentre los archivos del backup (estructura, full backup y incremental backup) y abrir la estructura (resaltado de rojo). Aparecera el nuevo Job en el servidor VEEAM BACKUP para ser ser seleccionado.

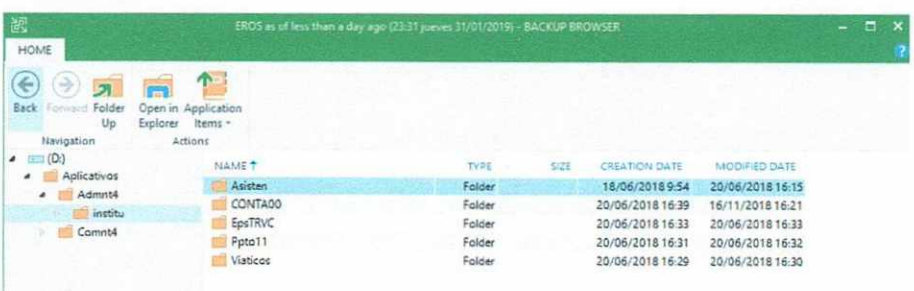


Nombre	Fecha de modifica...	Tipo	Tamaño
Backup Job EROS	31/01/2019 23:32	Veeam Backup & ...	220 KB
Backup Job EROS2019-01-19T233439	19/01/2019 23:51	Veeam Backup & ...	2.405.451 KB
Backup Job EROS2019-01-20T233033	20/01/2019 23:32	Veeam Backup & ...	46.070 KB
Backup Job EROS2019-01-21T233033	21/01/2019 23:32	Veeam Backup & ...	64.543 KB
Backup Job EROS2019-01-22T233033	22/01/2019 23:32	Veeam Backup & ...	129.293 KB
Backup Job EROS2019-01-23T233033	23/01/2019 23:32	Veeam Backup & ...	146.358 KB
Backup Job EROS2019-01-24T233033	24/01/2019 23:32	Veeam Backup & ...	113.319 KB
Backup Job EROS2019-01-25T233033	25/01/2019 23:32	Veeam Backup & ...	137.589 KB
Backup Job EROS2019-01-26T233404	26/01/2019 23:50	Veeam Backup & ...	2.401.577 KB
Backup Job EROS2019-01-27T233032	27/01/2019 23:32	Veeam Backup & ...	46.486 KB
Backup Job EROS2019-01-28T233033	28/01/2019 23:32	Veeam Backup & ...	115.075 KB
Backup Job EROS2019-01-29T233033	29/01/2019 23:32	Veeam Backup & ...	139.171 KB
Backup Job EROS2019-01-30T233033	30/01/2019 23:32	Veeam Backup & ...	48.951 KB
Backup Job EROS2019-01-31T233032	31/01/2019 23:32	Veeam Backup & ...	115.237 KB

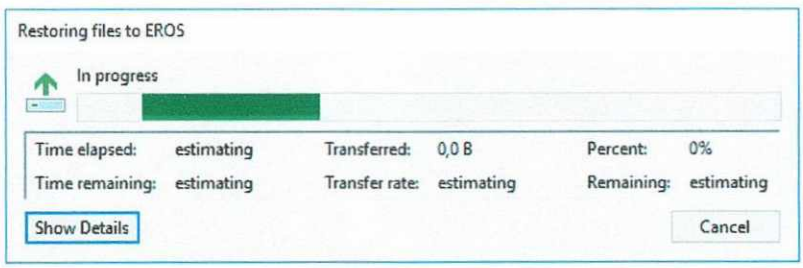
En la ventana de "Restore Point" de saldra la lista de los backups realizados, y se debe elegir al que se quiera restaurar.



Lo siguientes pasos mostraran si se quiere ingresar alguna razón (opcional) y por último el resumen, al finalizar se abrirá otra ventana:



En esta ventana puede elegir archivos especificos de todo el backup realizado, y tiene la opcion de restaurarlo, en el mismo sitio o en alguna direccion distinta.



Con eso se termina la restauración de una copia de respaldo.

Trabajando para ti
EPS
Entidad Prestadora de Servicios de Saneamiento TACNA S.A.

EPS TACNA S.A.
GERENCIA GENERAL
24 DIC 2021
Registro: 5864
Hora: Firma:

INFORME Nº 169-2021-450-EPS TACNA S.A

A : ING. JUAN ALBERTO SEMINARIO MACHUCA
GERENTE GENERAL

ASUNTO : APROBACION PLAN DE CONTINGENCIA Y SEGURIDAD DE LA INFORMACION

FECHA : Tacna, 24 de Diciembre del 2021

Es grato dirigirme a Ud, para saludarlo cordialmente, y remitir a su despacho el Proyecto de Plan de Contingencia y Seguridad de la Información, ha sido elaborado en base a:

- La ley Nº 28551, que establece la obligación de elaborar y presentar Planes de contingencia.
- La ley Nº 28716 "Ley de control interno de las Entidades del Estado"

El mismo que debe ser aprobado con Resolución de Gerencia General, con el fin de poner en conocimiento de todos los involucrados, se adjunta Proyecto de Resolución.

Atentamente,

EPS TACNA S.A.
Ing. EDUARDO S. CHOQUE CHACOLLA
CIP 101550
Jefe Ofic. Tecnología de la Información

Se Adjunta:
1. Plan de Contingencia y Seguridad de la Información
2. Plan de Backup
3. Proyecto de Resolución

c.c. Archivo

E. P. S. TACNA S.A.
Gerencia General
Proveído Nº ..... Fecha: 24 DIC 2021
Dirigido a: S.G.E.
Asunto: Para su Trámite
.....
.....
.....

Entidad Prestadora de Servicios de Saneamiento TACNA S.A. GERENCIA GENERAL Tacna S.A.

Av. Dos de Mayo N° 372 – Tacna
Telf. (052) 583446 – Fax (052) 583453
Mail: eps.informes@epstacna.com.pe