ADAMANTINE

Disaster Recovery Plan

Control de cambios

Fecha de Cambio	Estatus	Nombre	Versión	Descripción de cambios
3 Febrero 2020	Terminado	Gerardo Butrón Arnold Viveros Edith Paredes	V1	Creación de documento
7 Agosto 2020	Terminado	Edith Paredes	V2	• Tiempos de recuperación RPO y RTO • Protocolo de Activación de la arquitectura tecnológica • Roles de Equipo de Crisis

Origen: Ciudad de México

Contenido

Introducción

Con la finalidad de que Adamantine cuente con una estrategia y acciones para seguir las operaciones del negocio, se implementó el Plan de DR para restablecer los servicios de TI ante cualquier eventualidad en tiempos cortos y sin pérdida de información.

El objetivo de este DRP es reducir al máximo los efectos de un desastre en las funciones de Adamantine, para ser capaces de reanudar rápidamente sus funciones.

En este DR se contempla:

- Desarrollo de una estrategia de recuperación y continuidad del negocio.
- Concientizar, capacitar y probar el plan de DR
- Mantener y mejorar el plan de recuperación ante desastres
- Definir los tiempos de recuperación RTO y RPO
- Pruebas periódicas del DR con el equipo de recuperación y obtener evidencias
- Reuniones periódicas para revisión del plan DR
- Mantener vigente el sitio alterno en caso de un desastre

Misión

Contar con un plan estratégico en caso de un desastre provocado por el hombre, un evento natural o cualquier otro que impida la operación de TI en el Data Center principal de Adamantine.

Visión

Resolver los posibles eventos de riesgos y poder continuar con la operación de la empresa, de acuerdo con el tiempo de recuperación que defina la compañía.

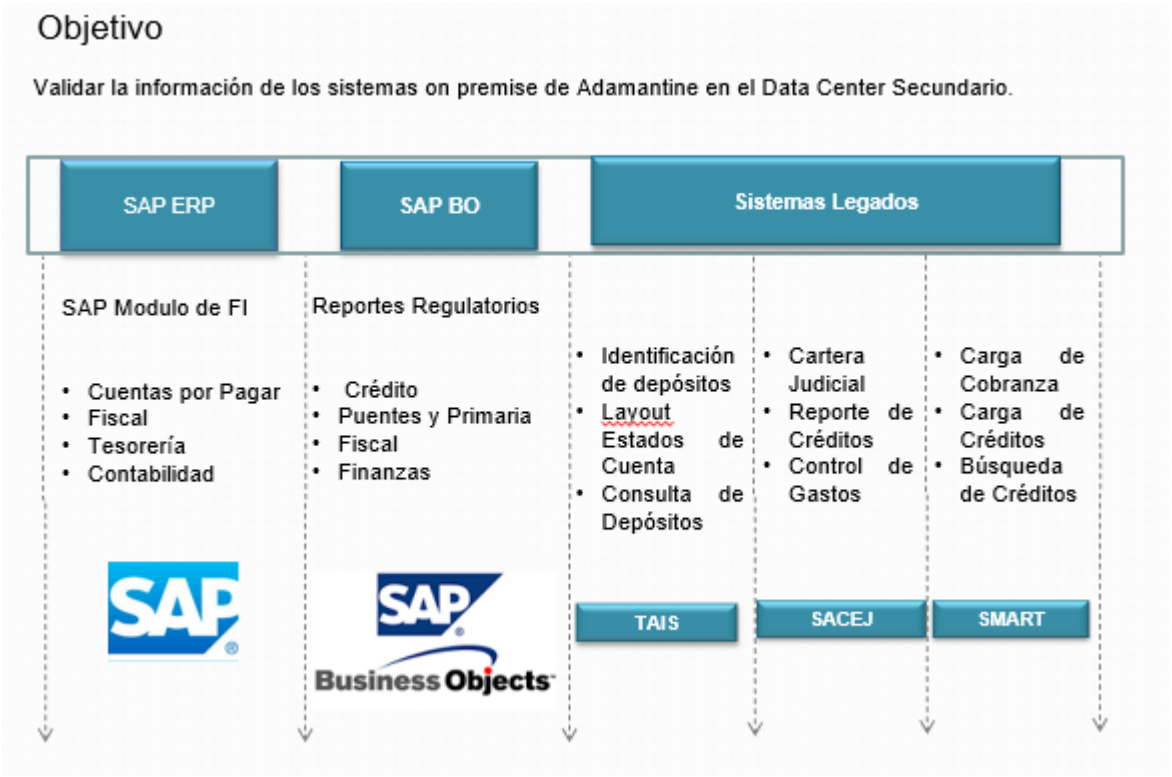
Audiencia del Documento

Este documento de DR está destinado para su uso de cualquier persona que tenga los permisos necesarios en los sistemas de Adamantine, así poder restaurar los sistemas en un tiempo definido.

Objetivos del Documento

Los objetivos del documento son:

- Exponer el diseño e implementación de una Estrategia de Continuidad de la arquitectura tecnologica que proteja y asegure la información en caso de una contingencia.



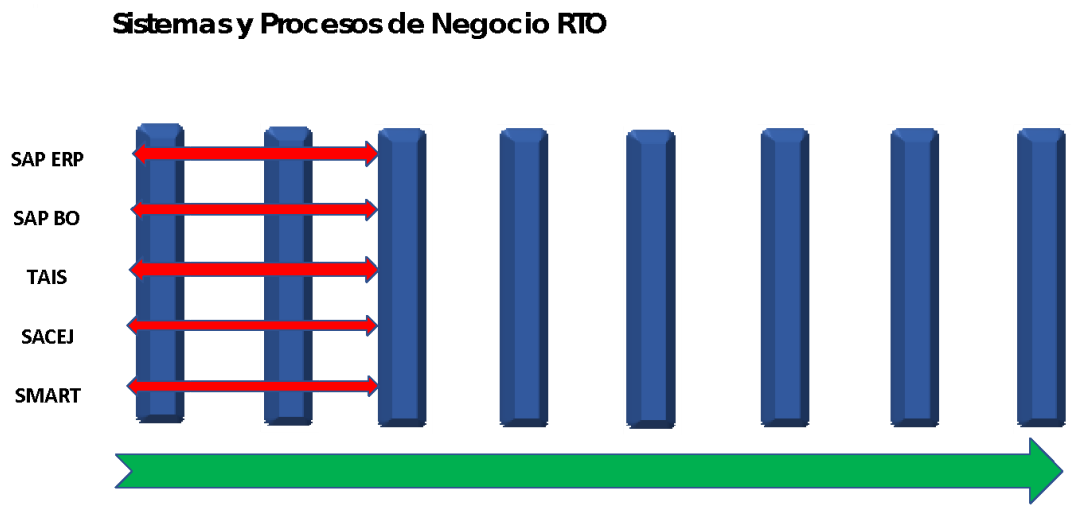
Alcance de este plan

Se limita a los aplicativos, máquinas virtuales y BD que viven en el Site de Adamantine onpremise. Todos los aplicativos que sean por terceros (SaaS) se solicitara anualmente evidencias que demuestre que continuar con el servicio brindado a Adamantine en una situación de contingencia

Características de la solución

Implementación de una herramienta de respaldos que nos permita restablecer la operación con el minino impacto y en un tiempo adecuado, en diversos escenarios con alojamiento en nube privada y la publicación de su aplicación.

Tiempos de recuperación RPO y RTO



Proceso de Declaración de contingencia

Recovery Point Objetive (RPO) 24 horas

Punto en el tiempo hasta el cual será posible recuperar el registro de la información y las aplicaciones

Recovery Time objective (RTO) 24 horas

Intervalo de tiempo requerido para recuperar los sistemas e información

Protocolo de Activación de la arquitectura tecnológica

La activación de pruebas DRP se llevó a cabo con los siguientes pasos ejecutados:

ID	Actividad
1	El Ingeniero de Infraestructura detecta la contingencia y notifica al Gerente de Infraestructura (correo electrónico)
2	El Gerente de Infraestructura notifica Director de Sistemas sobre la contingencia del desastre. (correo electrónico)
3	El director de Sistemas notifica al Comité de Manejo de Crisis (Dir. General, Dir. Auditoria) sobre el desastre (correo electrónico)
4	El Director General da su VoBo para ejecutar el DRP a la Dir. de Sistemas y equipo (correo electrónico)
5	Gerente de Infraestructura notifica al equipo de recuperación de desastres TI la activación del DRP (correo electrónico)
6	El equipo de Ingeniería del Site Alterno confirma que está enterado del evento de contingencia (correo electrónico) y que procederá con la ejecución del DRP.
7	El equipo de Ingeniería del Site Alterno, valida los recursos de hardware en la infraestructura de virtualización Cloud y envía un estatus (correo electrónico).
8	El equipo de Ingeniería del Site Alterno envía al Gerente de Infra la validación de los respaldos a restaurar (correo electrónico)

9	Gerente de Infraestructura revisa con Dir. Sistemas y Dir. Auditoria y confirma al equipo de Ingeniera del Site Alterno los respaldos a restaurar (correo electrónico)
10	Se solicita al Gerente de Infraestructura ingrese la contraseña de protección del respaldo para ejecutar la restauración de los servidores (remotamente)
11	Inicia el proceso de restauración en el Data Center Alterno y se notifica (vía correo electrónico) al Gerente de Infraestructura
12	Al finalizar el proceso de restore, se notifica la disponibilidad del 100% al Gerente de Infraestructura para su validación (vía correo electrónico)
13	El Gerente de Infraestructura notifica al comité de crisis, los consultores funcionales para su validación y los usuarios clave para iniciar la prueba de DRP (vía correo electrónico)
14	Los usuarios clave inician sus pruebas (ya cuentan con credenciales y scripts de pruebas)
15	Finaliza la prueba de DRP, se realiza la entrega de evidencias y scripts de pruebas por parte de los usuarios (vía correo electrónico)
16	Se realiza la validación de la información, se firmas los documentos (anexar correos electrónicos de usuarios) y Carta de finalización de pruebas

Ubicación Adamantine

Av. Insurgentes Sur 1647, San José Insurgentes, Benito Juárez, 03900 Ciudad de México, CDMX. Las oficinas se encuentran en el piso 5 .

PISO 5

Ubicación del proveedor de Sitio Alterno DR - Sittec

Equipo de Manejo de Crisis

Puesto	Nombre	Rol	Correo
Director General	Lic. Sergio Carrera Dávila	Toma las decisiones de la activación del DRP. En Adamantine Gestiona las actividades de la organización estableciendo tareas, objetivos y prioridades.	sc@adamantine.com.mx
Director de Recursos Humanos	Lic. Luis Felipe Flores Sánchez	Ofrece orientación y comunicación en la compañía. Toma decisiones dentro del comité de crisis.	lffloress@adamantine.com.mx
Director de sistemas	Ing. Juan Francisco Torres	Coordinar todas las actividades de la prueba de DRP, es decir, supervisan el desempeño del equipo de sistemas, establecen los objetivos del evento.	ftorres@adamantine.com.mx
Director de Auditoria	Lic. José Luis Dávila Becerril	Supervisa la eficiencia, y desempeño del DRP, asegurando el cumplimiento de esta. Realiza recomendaciones	jldavila@adamantine.com.mx

		dentro del comité de crisis.	

Responsables del área de sistemas TI Adamantine

Puesto	Nombre	Rol	Correo
Director de sistemas	Ing. Juan Francisco Torres	Responsable del área de sistemas y dar seguimiento puntual del proceso del DRP	ftorres@adamantine.com.mx
Gerente de Infraestructura	Ing. Gerardo E. Butron Medina	Dar cumplimiento al DRP, gestionar la infraestructura interna y en el DRP de Adamantine.	gebutron@adamantine.com.mx

Administradores de sistemas críticos Adamantine

Sistema	Nombre	Rol	Correo
SAP FI	Jheannary Paola Dufflart Hdz.	Responsable del modulo de Finanzas en el ERP de Adamantine	jdufflart@adamantine.com.mx
SAP BASIS	Edith Paredes Ramírez	Responsable de administrar el sistema ERP de Adamantine	eparedes@adamantine.com.mx
SAP BO	Victor A. Rueda Santos	Responsable de la administración del sistema de reportes regulatorios.	vrueda@adamantine.com.mx
SQL&IIS	Gerardo Flores	Responsable de los sistemas desarrollados internamente (legados)	gflores@adamantine.com.mx

Contactos de proveedor de servicios en la nube

Puesto	Nombre	Contacto	Correo
Director General	C.P Eric Ramos Vázquez	Cel. 5519509933 56744846 ext. 102	eric.ramos@sittec.net

Gerente de Ingeniería	Ing. Adrián Beltrán Salas	Cel. 5567901091 56744846 ext. 110	adrian.beltran@sittec.net
Ingeniero en Soluciones TI	Ing. Emanuel López Chávez	Cel. 5577878523 56744846 ext. 102	emanuel.lopez@sittec.net
Gerente Administrativo	Araceli López Ramos	Cel. 5527529485 56744846 ext. 103	araceli.lopez@sittec.net
Atención a Clientes	Marlene Ramos Vargas	Cel. 5556090457 56744846 56744856	info@sittec.net

Matriz de escalación

Nivel de escalación	Puesto	Nombre
1	Ingeniero en Soluciones TI	Ing. Emanuel López Chávez
2	Gerente de Ingeniería	Ing. Adrián Beltrán Salas
3	Director General	C.P Eric Ramos Vázquez

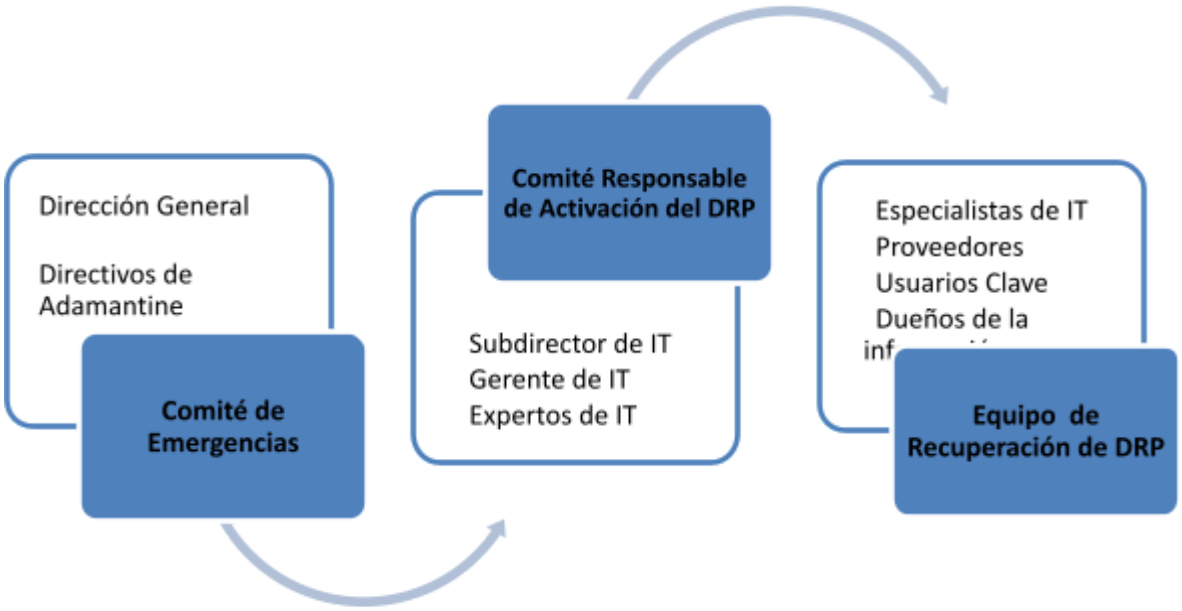
Comité DRP

Comité de Emergencias: este equipo de emergencias es definido internamente por Adamantine, es el responsable de la activación de la contingencia, notifica al Comité responsable de la Activación del DRP.

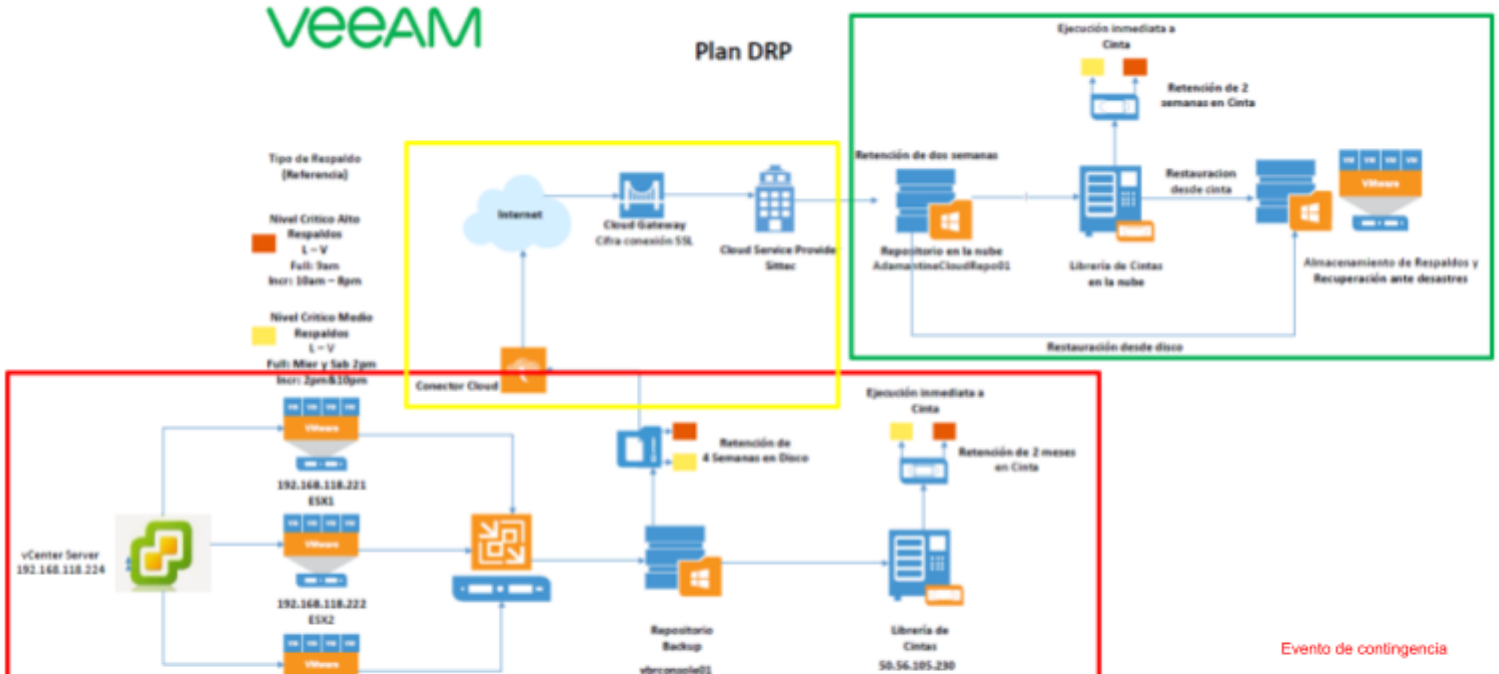
Comité responsable de activación DRP: se encuentra conformado por los responsables de la activación del plan de recuperación de desastres DRP, notifica al Equipo de Recuperación de DRP para que inicie el proceso de DR.

Equipo de Recuperación DRP: Incluye todo el personal del área de tecnología de Adamantine, los proveedores y los usuarios claves de la compañía, son los encargados de realizar la activación de los servicios definidos como críticos y la puesta en funcionamiento de los sistemas contemplados dentro del alcance del DRP.

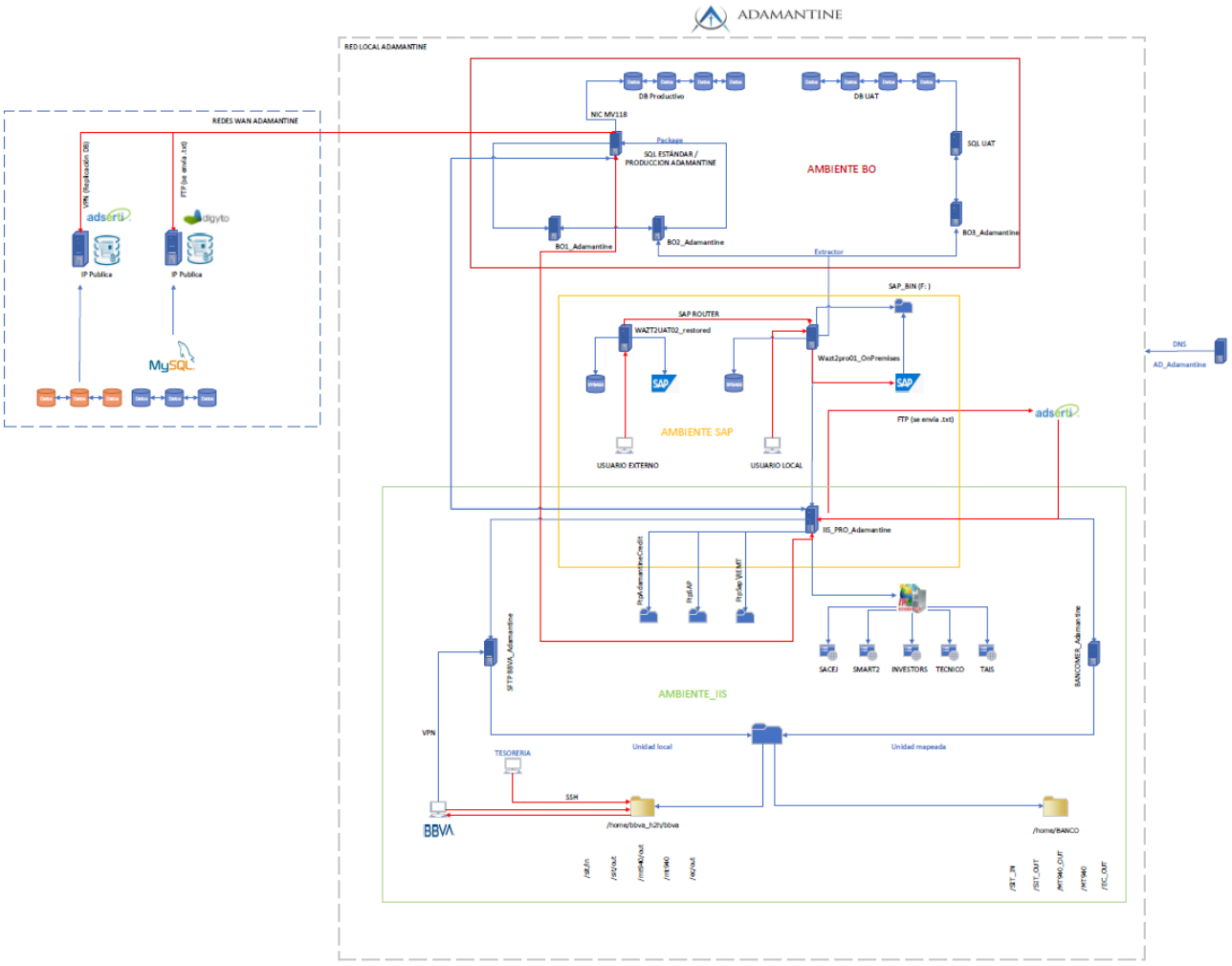
ADAMANTINE



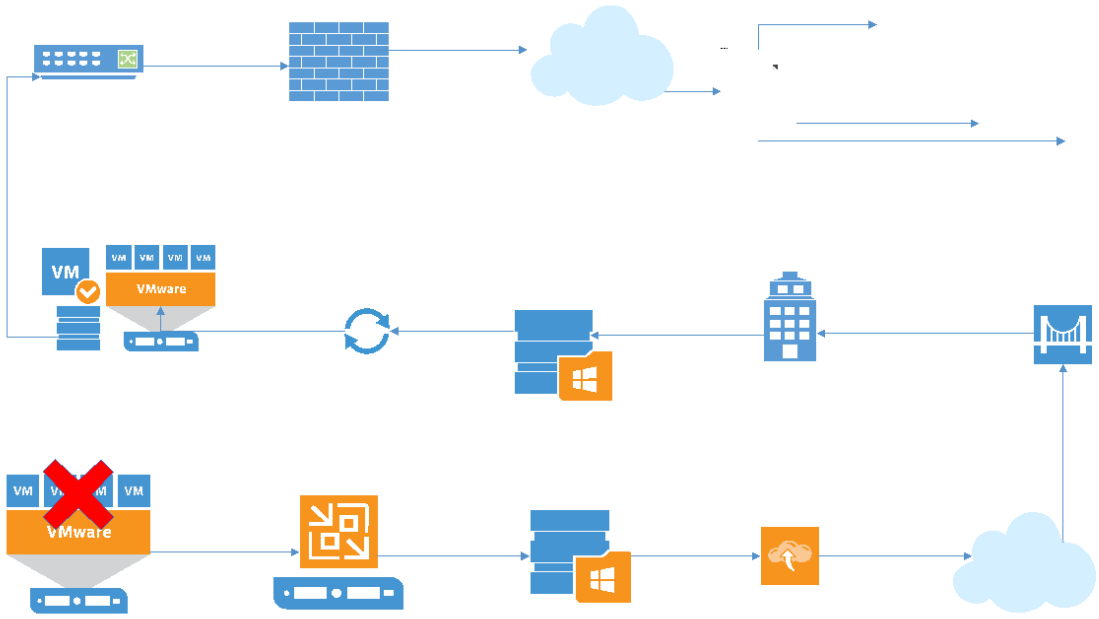
Arquitectura general de plan de restauración ante desastres



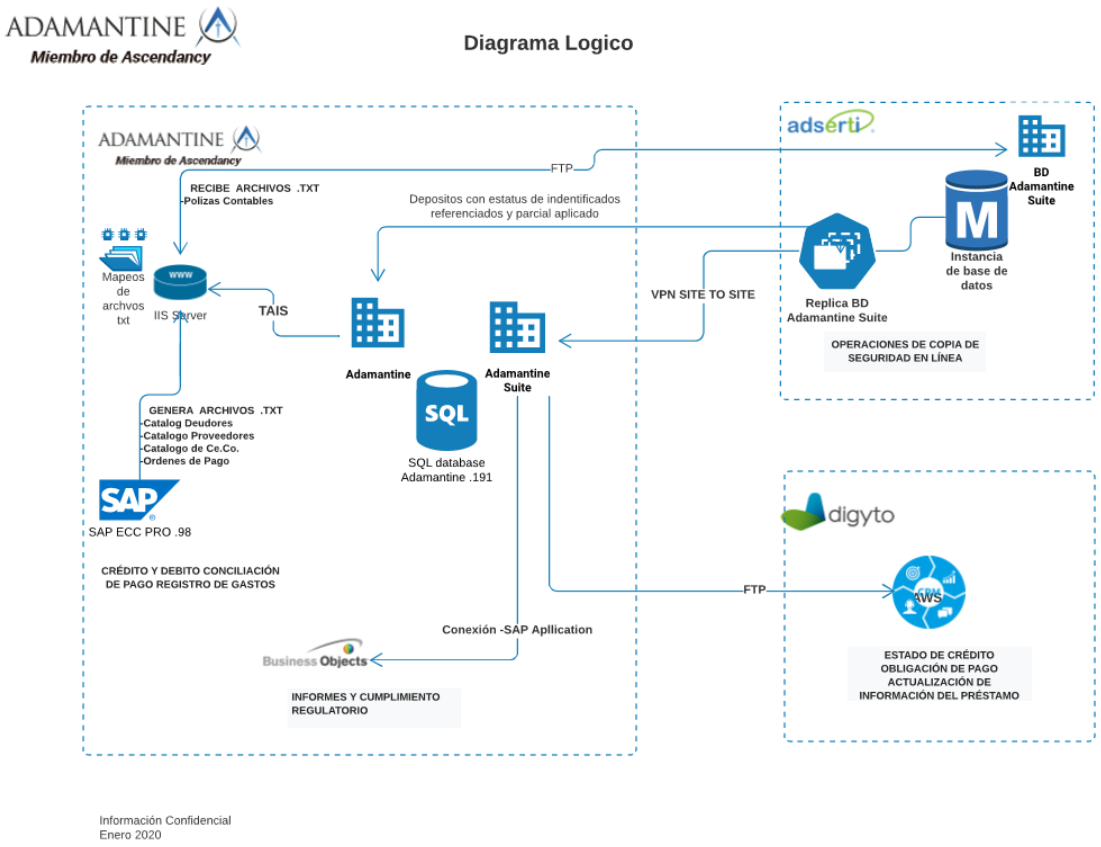
Arquitectura general de ambientes productivos Adamantine



Arquitectura para publicación de aplicaciones en infraestructura Citrix Cloud



Arquitectura de sitios WEB y CRM Adamantine



Información Confidencial
Enero 2020

Esquema de respaldos de ambientes productivos

A continuación, se enlistan las máquinas virtuales productivas críticas involucradas en el plan de recuperación ante desastres.:

Servidor Virtual	Criticidad	Job a dico	Job a la nube
AD_Adamantine	Alta	Serv_Prod_Back	Serv_Diario_Cloud_Back
B01_Adamantine	Alta	BO_Back	BO_Cloud_Back
B02_Adamantine	Alta	BO_ Back	BO_Cloud_Back
IIS_PRO_Adamantine	Alta	IIS_PROD_Back	Serv_Prod_Back
BANCOMER_Adamantine*	Alta	BANCOS_PROD_Back	BANCOS_Cloud_Back
SFTP BBVA_Adamantine*	Alta	BANCOS_PROD_Back	BANCOS_Cloud_Back
SQL STANDAR / PRODUCCION_ADAMANTINE	Alta	SQL_Back	SQL_PROD_CloudJob
wazt2pro01_OnPremises	Alta	SAP_Prod_Back	SAP_Prod_Back_CloudJob

Como se puede observar en la tabla, las VM´s con criticidad alta se debe a que de ellas dependen los ambientes productivos que integran sistemas, aplicativos, sitios WEB y otras soluciones. En caso de que alguna de ellas falle, la disponibilidad de procesos o servicios se verá afectada hasta su restauración en la nube. En Adamantine se tiene tres ambientes productivos:

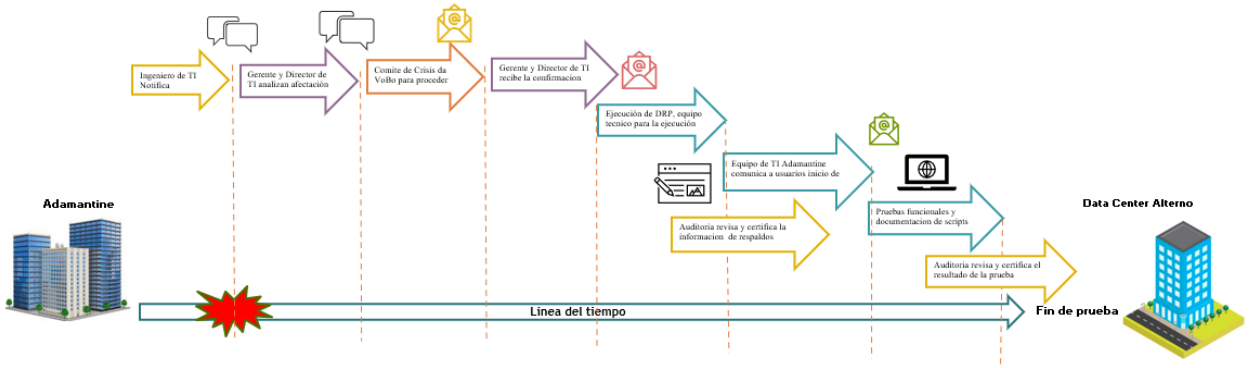
- SAP ERP (SAP)
- SAP Business Objects (BO)
- Sitios WEB (IIS)

Plan de recuperación ante desastres (DRP)

Se realizarán los ejercicios completos correspondientes al plan de recuperación ante desastres de los ambientes considerados como críticos (SAP, BO y IIS) para garantizar la continuidad del negocio.

- **El tiempo de espera para activar el plan DRP será de 24 horas**
- La restauración DRP de los sistemas TI Adamantine debe realizarse en un lapso no mayor a **24 horas**. Dicho tiempo inicia a partir de que los responsables del área de sistemas dan aviso que se ha presentado el evento de contingencia.

Es importante garantizar que a pesar de que no exista un evento real de contingencia, la restauración de la operación es posible con la mínima pérdida de información y en el menor tiempo posible.



RTO	24 horas
RPO	24 horas

Sanidad de los archivos de respaldo

Se garantizará que los respaldos se están realizando correctamente, debe configurarse la ejecución de “SureBackup” los domingos de cada semana.

La ejecución de estos Jobs permitirá comprobar, validar y demostrar la recuperabilidad desde cualquier punto de restauración en un entorno aislado. Para realizar la verificación de la recuperabilidad, Veeam DataLabs inicia automáticamente la VM en un entorno aislado antes de ejecutar una serie de pruebas predefinidas como una prueba de latido, networking y estado de aplicación para garantizar el correcto funcionamiento. Al finalizar, deben notificarse vía correo electrónico los resultados obtenidos.

Integridad de los archivos de respaldo

Se garantizará la integridad de los archivos de backup, se realizarán dos “Virtual Labs” en la nube los meses de marzo y octubre del presente año para realizar validaciones específicas en cada máquina virtual (red, unidades locales, tareas programadas, aplicativos, etc.) con el apoyo de los administradores de los sistemas. Una vez que se finaliza el laboratorio, la VM es apagada descartando todos los cambios durante la prueba y entonces debe enviarse un informe de estado del backup.

Adicional, los laboratorios:

- Proporcionan confianza a la organización mientras mejora las eficiencias operativas al comprobar la capacidad de recuperación de cada backup

- Los administradores de sistemas pueden usar este método en modo para poner en marcha instancias aisladas de un entorno de producción para diseñar y probar nuevas funciones de forma continua antes de implementarlas en el entorno de producción, todo ello sin interrumpir la red o requerir más almacenamiento.
- Probar nuevos parches y actualizaciones en un entorno antes de pasarlos a producción, para reducir el impacto en el entorno de producción mientras impulsa una estrategia de pruebas y desarrollo.

Consideraciones de restauración en la nube

El área de TI en Adamantine tienen la responsabilidad de informar de la presencia de un evento crítico que implica ejecutar el plan DR en las instalaciones del proveedor de respaldos en la nube proporcionando y garantizando la siguiente información:

- Ambiente involucrado
- Configuración de dirección IP de la VM (privada y pública)
- Procesos y servicios de las VMs
- Criticidad
- Identificar el Job de respaldo en la nube al que pertenece la(s) VM
- Fecha y hora en que se presentó la contingencia
- Definir el punto de restauración de la VM dadas las condiciones
- Establecer canales de comunicación con el administrador del sistema durante el proceso de restauración para realizar las pruebas y validaciones correspondientes
- Es necesario que los responsables del área de TI ingresen remotamente la contraseña de protección del respaldo para realizar la restauración.
- Mantener actualizado los respaldos en la nube
- Alta disponibilidad del enlace dedicado a la transferencia de respaldos
- Antivirus Sophos*

Proceso de restauración ante desastres

El punto crítico de las actividades de recuperación es que se garantice que el sistema de respaldos local y el sistema de respaldos en la nube se encuentren en sincronía en todo momento para minimizar la perdida de información y disponer de un punto de restauración cercano.

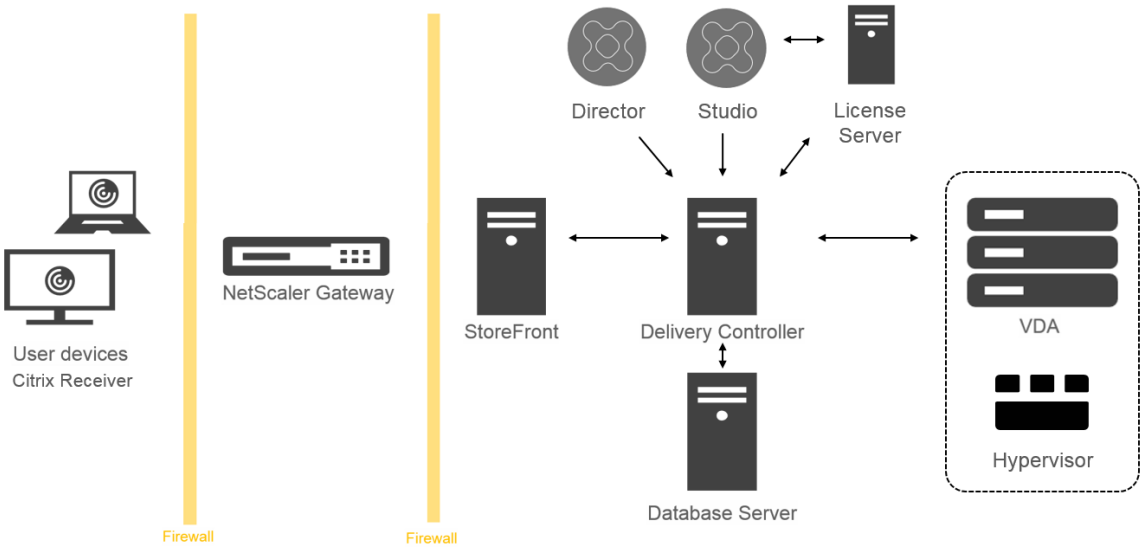
Cuando se presenta un evento de contingencia que no permite recuperar la operación On-Premise es necesario ejecutar el plan DRP en la nube como se describe a continuación.

1. Desde la consola de administración Veeam Backup de los sistemas de respaldos en la nube debe seleccionarse la opción de Restaurar la máquina completa desde un archivo de respaldo (punto de restauración específico).
2. Para proceder con la restauración de la VM, los responsables del área de IT de Adamantine deben ingresar remotamente la contraseña de protección del respaldo almacenado en el repositorio en la nube.
3. Al ser una restauración FULL, debemos esperar a que el archivo de respaldo se transfiera por completo al Storage de producción de la infraestructura de virtualización de VMware.
4. El entorno de vCenter Server permitirá encender la máquina para ultimar detalles de configuración.
5. Ingresamos a la VM para realizar pruebas y validaciones de su funcionamiento.
6. Publicación de las aplicaciones en Citrix*

Publicación de aplicaciones en Citrix

Una vez que se ha validado el funcionamiento de los sistemas y aplicaciones en la nube privada, debe darse acceso a ellas a los usuarios que se definan en un plan de contingencia.

Citrix receiver nos permitirá acceder a dichos entornos desde cualquier parte, sin importar el hardware que estemos usando, ahorrando costes y reforzando la seguridad al ofrecer un entorno estandarizado.



La virtualización de aplicaciones y escritorios permite ejecutar una aplicación desde un dispositivo en el que no está instalada. El objetivo de esta virtualización es conseguir que las aplicaciones y equipos puedan funcionar con independencia de las características concretas del entorno en que se ejecutan. Además, podemos utilizar casi cualquier dispositivo como móviles o tabletas, en cualquier momento y desde cualquier lugar.

Sistema de respaldos y restauración Adamantine

- **Firewall Perimetral Fortigate 500E – HA**

Un clúster HA activo-pasivo (AP): Un clúster activo-pasivo consiste en una unidad primaria que procesa sesiones de comunicación y una o más unidades subordinadas. Las unidades subordinadas están conectadas a la red y a la unidad primaria, pero no procesan sesiones de comunicación. En cambio, las unidades subordinadas se ejecutan en estado de espera. En este estado de espera, la configuración de las unidades subordinadas se sincroniza con la configuración de la unidad primaria y las unidades subordinadas monitorean el estado de la unidad primaria.

La HA activa-pasiva proporciona una conmutación por error transparente del dispositivo entre las unidades de clúster. Si una unidad de clúster falla, otra inmediatamente toma su lugar.

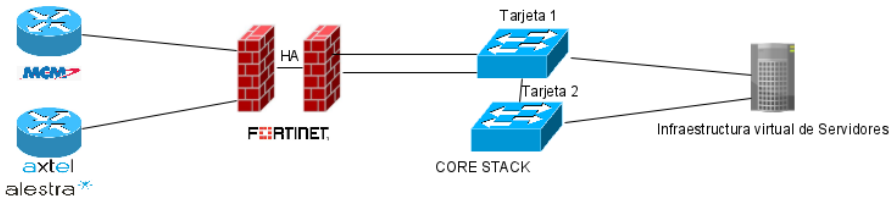
La HA activa-pasiva también proporciona conmutación por error de enlace transparente entre unidades de clúster. Si una interfaz de unidad de clúster falla o se desconecta, esta unidad de clúster actualiza la base de datos de estado de enlace y el clúster negocia y puede seleccionar una nueva unidad primaria.

Si la conmutación por error de sesión (también llamada recuperación de sesión) está habilitada, la HA activa-pasiva proporciona conmutación por error de sesión para algunas sesiones de comunicación.

- **Switch Core Cisco – Stack**

La tecnología Cisco StackWise-480 se basa en la exitosa tecnología StackWise, líder en la industria, que es una arquitectura de apilamiento Premium. StackWise-480 tiene un ancho de banda de pila de 480 Gbps. StackWise - 480 utiliza el SSO de Cisco IOS Software para proporcionar resistencia dentro de la pila. La pila se comporta como una sola unidad de conmutación que es administrada por un miembro "activo" elegido por los miembros dentro de la pila.

El switch activo elige automáticamente un switch de espera dentro de la pila. El miembro activo crea y actualiza toda la información de conmutación / enrutamiento / inalámbrica y sincroniza constantemente esa información con el miembro de espera. Si el switch activo falla, el miembro en espera asume la función del switch activo y continúa para mantener la pila operativa. Los puntos de acceso siguen estando conectados durante un cambio activo a modo de espera.



- **Redundancia en salida a Internet (SDWAN)**

La SD-WAN es una arquitectura de red de área extensa definida por software que permite a las organizaciones modernizar sus redes WAN tradicionales para satisfacer los crecientes requerimientos de la evolución digital.

Con las soluciones de SD-WAN, las organizaciones obtienen capacidades de red de alto rendimiento compatibles con las iniciativas de transformación digital (DX) para simplificar las operaciones y mejorar la agilidad empresarial.

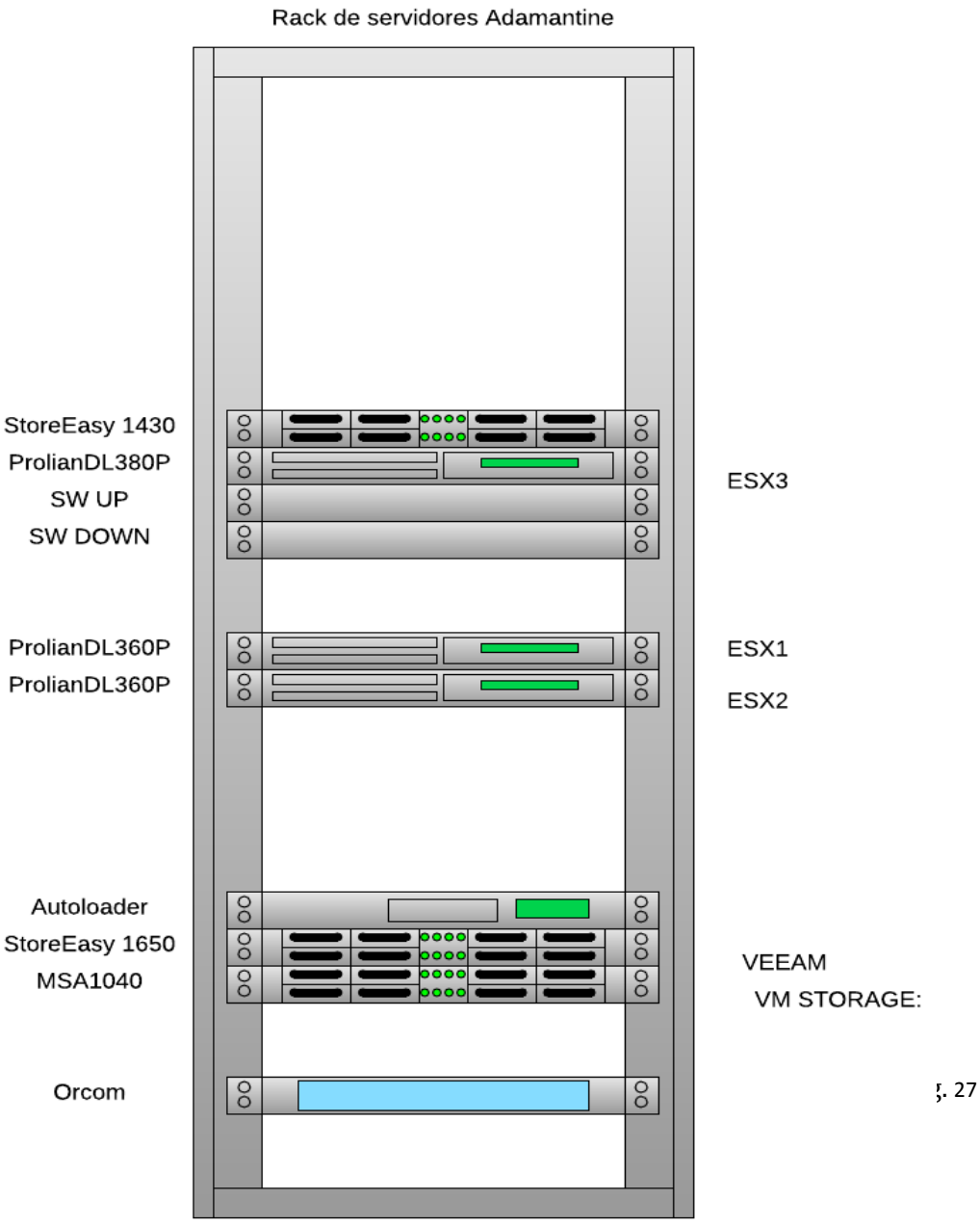
Infraestructura virtual de servidores On-Premise

La infraestructura virtual de Adamantine está integrado en un vCenter Server Appliance (VCSA). Administra tres servidores ESXI de VMware, en donde se crean las máquinas virtuales y proveen los recursos físicos de dichas VM´s.

vCenter Server Appliance proporciona alta disponibilidad, migración de servidores y planes de recuperación provocados por los equipos de infraestructura. Para garantizar estas características, los servidores ESXI comparten una unidad de almacenamiento MSA 1040 SAN y de esta forma acceder a los recursos de los otros hosts.

- Servidor ESX1 Adamantine, VMware 6.0.0, 3620759
- Servidor ESX2 Adamantine, VMware 6.0.0, 3620759
- Servidor ESX3 Adamantine, VMware 6.0.0, 3620759
- vCenter Server Appliance, VMware 6.7.0.10000 (virtual)
- StoreEasy 1430 Storage, STORAGE-HP1-8TB
- StoreEasy 1650 Storage, STORAGE-HP-50TB
- Autoloader 1x8 G2, x2 magazine
- MSA 1040 SAN, HP-30TB

- Switch FI Up
- Siwtch FI Down
- Infraestructura de red: VLAN
- Infraestructura de seguridad: FIREWALL FG



Factores de riesgo

Existen factores que pueden afectar la continuidad de la operación de sistemas y servicios que provee Adamantine por desastres naturales, fallas en los sistemas del edificio (eléctricos, estructuras, aire acondicionado, etc.), accidentes (incendio, fuga de gas, etc.) o falla en los equipos de la infraestructura de red, virtual o de otro tipo.

- Desastre Natural

Los desastres naturales son una variable existente y recurrente que interrumpen las actividades económicas, políticas y sociales. En Adamantine son conscientes que la disponibilidad, integridad y continuidad del negocio son lo más importante para ofrecer servicios a los clientes en todo momento.

- Acceso al corporativo

Existen factores que pueden impedir el acceso al edificio causados por desastres naturales, accidentes o problemas en la infraestructura que ponen en riesgo la vida de los usuarios y, por lo tanto, afectar la operación de los sistemas de la empresa.

- Equipos de infraestructura

Uno de los problemas más probables en el área de sistemas es causado por fallas en el hardware de los equipos que soportan la operación de la infraestructura de IT.

- Error humano

Es uno de los problemas más comunes y de mayor índice en las empresas. Se debe a la mala operación de los equipos o configuraciones mal ejecutadas en el hardware o software, derivado de la operación diaria de los administradores de sistemas.

Tipos de fallas

La operación diaria de los sistemas que soporta la infraestructura de Adamantine es susceptible a eventos de fallas que por su criticidad se tienen diferentes escenarios de afectación. A continuación, se enlistan las tres principales:

a) Parcial: Su afectación es transparente en la operación debido a que se cuentan con técnicas y métodos de redundancia en la configuración de los equipos de red,

almacenamiento, de virtualización, seguridad y otros para garantizar alta disponibilidad ante fallas capa 1.

b) Temporal: Este tipo de falla puede tener como consecuencia afectaciones de mayor trascendencia. Puede fallar un host de virtualización, enlace ISP, sistema operativo de una VM, problemas de red en la intranet, sistema de energía, otros.

c) Permanente: Este tipo de problemas puede considerarse critico si se define que la restauración de la operación de los sistemas en la infraestructura local no es posible. Es en este punto cuando debe aplicarse el plan de recuperación ante desastre (DRP) en la nube.

- Falla parcial

Las fallas parciales en la infraestructura se pueden soportar con los equipos disponibles localmente. Los equipos están configurados para ofrecer:

- Redundancia de red
- Redundancia de energía
- Redundancia de almacenamiento (RAID)
- Alta disponibilidad* y tolerancia a fallas (Infraestructura virtual)

Todos los equipos cuentan con una suscripción de garantía activa en sitio con los proveedores por falla en hardware o de software.

- Falla temporal

Las fallas temporales tienen un grado de complejidad más grande porque depende de la operación de terceros como lo son los proveedores de internet y proveedores de equipos en garantía. Además, los administradores de sistema IT deben encontrar la raíz del problema y elaborar un plan de recuperación en la infraestructura local en el menor tiempo posible.

Cuando un equipo presenta una falla que no es soportada por su redundancia, causara problemas en todos los niveles de la operación con tiempos de recuperación no estimados. Dependiendo de la magnitud del problema *la cual se debe analizar en conjunto con los administradores de los sistemas, podemos restablecer localmente a la espera de solucionar la falla en un periodo de tiempo desconocido u optar por la restauración de los sistemas en la nube *falla permanente.

- Falla permanente

Una falla permanente puede considerarse de carácter critica cuando se define que la recuperación u operación On-Premise no es posible. Es momento de ejecutar el plan de recuperación ante desastres (DRP) en la nube con la disponibilidad de todas las partes para realizar pruebas y validaciones en los diferentes ambientes.

Es responsabilidad de ambas partes establecer protocolos de comunicación durante un plan de contingencia, así como la de discutir la mejor alternativa de solución.

Alta disponibilidad

Consiste en una serie de medidas tendientes a garantizar la disponibilidad del servicio, es decir, asegurar que el servicio funcione durante las veinticuatro horas.

Hight Availability VMware

Los servidores host de virtualización están configurados con High Availability (HA). VMware HA garantiza el reinicio de las máquinas virtuales en otro servidor ESX en caso de una caída o fallo del servidor físico.

Antes de configurar VMware HA, se verifico que todas las máquinas virtuales, pueden encenderse en los nodos que vayan a formar el clúster. Es importante el acceso a recursos comunes como LUN´s y redes virtuales para las máquinas virtuales. Todos los servidores ESX que forman parte del cluster HA deben ver las LUN's donde están las máquinas virtuales.

VMware HA, aunque es mínimo, hay downtime de las máquinas virtuales.

vMotion VMware

Cuando un servidor ESX presenta problemas de CPU, almacenamiento, memoria, etc. causados por diferentes factores, podemos realizar la migración de la(s) máquina virtual a uno que no presente afectaciones para evitar tiempos muertos de los ambientes productivos.

- En caliente, no implica reinicio de la VM
- En frío, implica reinicio y en consecuencia la afectación de sistemas y servicios.

Fallas en servidores virtuales

Cuando un servidor físico o virtual presente fallas en su sistema operativo causado por actualizaciones instaladas, configuraciones mal ejecutadas a un sistema, daños de archivos del sistema, que se eliminen o dañen ficheros raíz desde la infraestructura virtual y la VM no arranque será necesario realizar una restauración de la máquina.

Po ello, la importancia de un sistema de respaldos* y de restauración de VM´s es fundamental en el la operación de la empresa.

Sistema de respaldos

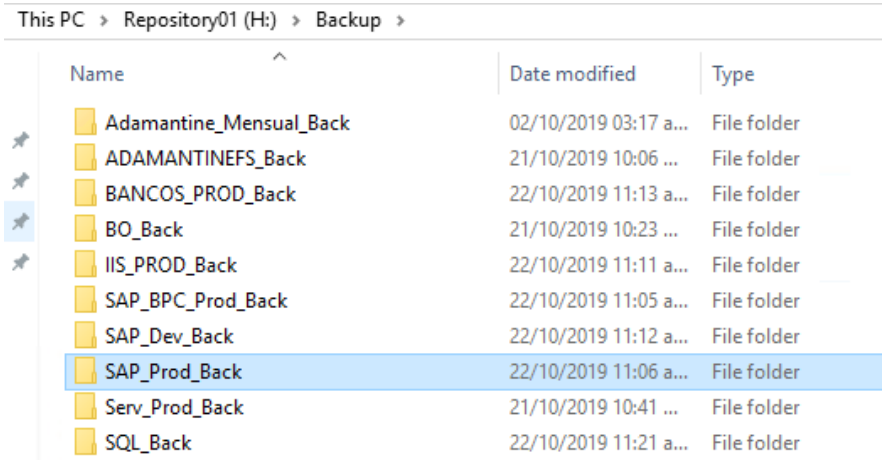
La regla 3-2-1 se volvió un concepto popular gracias a Peter Krogh, un fotógrafo conocido que escribió que hay dos tipos de personas: aquellas que ya han tenido una falla de almacenamiento y aquellas que tendrán una en el futuro. En otras palabras, la regla de backup 3-2-1 significa que debería:

- Almacenarlas en dos medios diferentes.
- Tener al menos tres copias de sus datos.
- Tener una copia de backup en un medio externo.

Sistema de respaldos Adamantine On-Premises

Las máquinas virtuales del Datacenter se almacenan en dos medios locales diferentes: cinta y disco.

Los respaldos a disco se realizan en un StoreEasy 1650 mapeado en el servidor de Veeam Backup & Replication (Repository01). Cada Job de respaldo crea una carpeta con el nombre del Job y en ella se van almacenando los archivos de respaldo completos (.vbk) e incrementales (.vib) de acuerdo con los tiempos de retención establecidos.



Los respaldos a cinta se realizan en unidades de cinta LTO-7 Ultrium RW de 5.5TB de capacidad. Una vez que el archivo de respaldo se encuentra en disco, se dispara inmediatamente el Job a cinta correspondiente. Los respaldos se almacenan en un pool de cintas, que deben cambiarse cuando llegan a su límite de capacidad.

Tiempo de retención en disco

El tiempo de retención en el Repositorio de Veeam es de 4 semanas. Por lo tanto, se puede restaurar una máquina virtual hasta este punto en el Datacenter Adamantine.

Tiempo de retención en cinta

El tiempo de retención de los archivos de respaldo de las VM a cinta es de dos meses, es decir, podemos restaurar un maquina hasta este punto. Para la operación de respaldos a cinta se reciclan las cintas HP LTO7 continuamente para tener disponibles todo el tiempo en futuros respaldos.

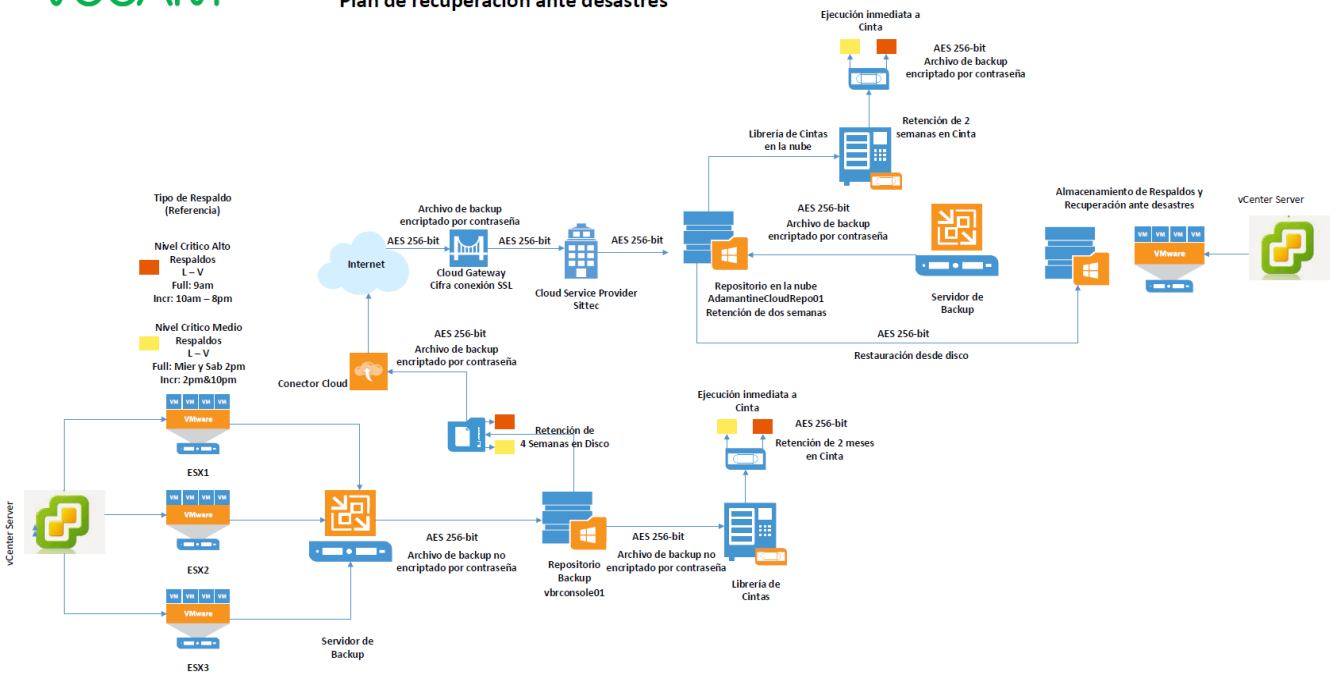
Ante una posible contingencia en las instalaciones de Adamantine, la primera opción de recuperación que debe buscarse es una restauración local completa (cinta o disco) de la(s) VM. De no ser posible, se procederá con el plan DRP Adamantine-Sittec.

Plan DRP: Sistema de respaldos Adamantine en la nube

Adicionalmente, se tiene una arquitectura de respaldo Backup Copy en la nube ubicada en las instalaciones del proveedor de virtualización Sistemas Técnicos de Información y Avance (Sittec).

NAME	TYPE	OBJECTS	STATUS	LAST RUN	LAST RESULT	NEXT RUN	TARGET
ADAMANTINEFS_Cloud_Back	VMware Backup Copy	1	Idle	9 hours ago	Success	<Continuous>	AdamantineCloudRepo01
BANCOS_Cloud_Back	VMware Backup Copy	2	Idle	11 hours ago	Success	<Continuous>	AdamantineCloudRepo01
BO_Cloud_Back	VMware Backup Copy	3	Idle	10 hours ago	Success	<Continuous>	AdamantineCloudRepo01
IIS_PROD_CloudJob	VMware Backup Copy	2	Idle	12 hours ago	Failed	<Continuous>	AdamantineCloudRepo01
SAP_BPC_Cloud_Back	VMware Backup Copy	1	Idle	13 hours ago	Failed	<Continuous>	AdamantineCloudRepo01
SAP_Dev_Cloud_Back	VMware Backup Copy	1	Idle	12 hours ago	Success	<Continuous>	AdamantineCloudRepo01
SAP_Prod_Back_CloudJob	VMware Backup Copy	1	Idle	13 hours ago	Success	<Continuous>	AdamantineCloudRepo01
Serv_Diario_Cloud_Back	VMware Backup Copy	7	Idle	2 hour ago	Failed	<Continuous>	AdamantineCloudRepo01
SQL_PROD_CloudJob	VMware Backup Copy	2	Idle	11 hours ago	Success	<Continuous>	AdamantineCloudRepo01

Los Backup copy son tareas programadas en la consola de administración local de respaldos de Veeam, que se ejecutan periódicamente y que realizan una copia del ultimo respaldo almacenado en el repositorio local, previo a la ejecución del Job. Dicho respaldo es enviado, cifrado* y encriptado por contraseña (protección del archivo de respaldo) a un repositorio en la nube (AdamantineCloudRepo01) a través de internet por un enlace simétrico dedicado de 100MB mediante. El tiempo de retención de los Backup en la nube es de dos semanas, para disco y cinta.

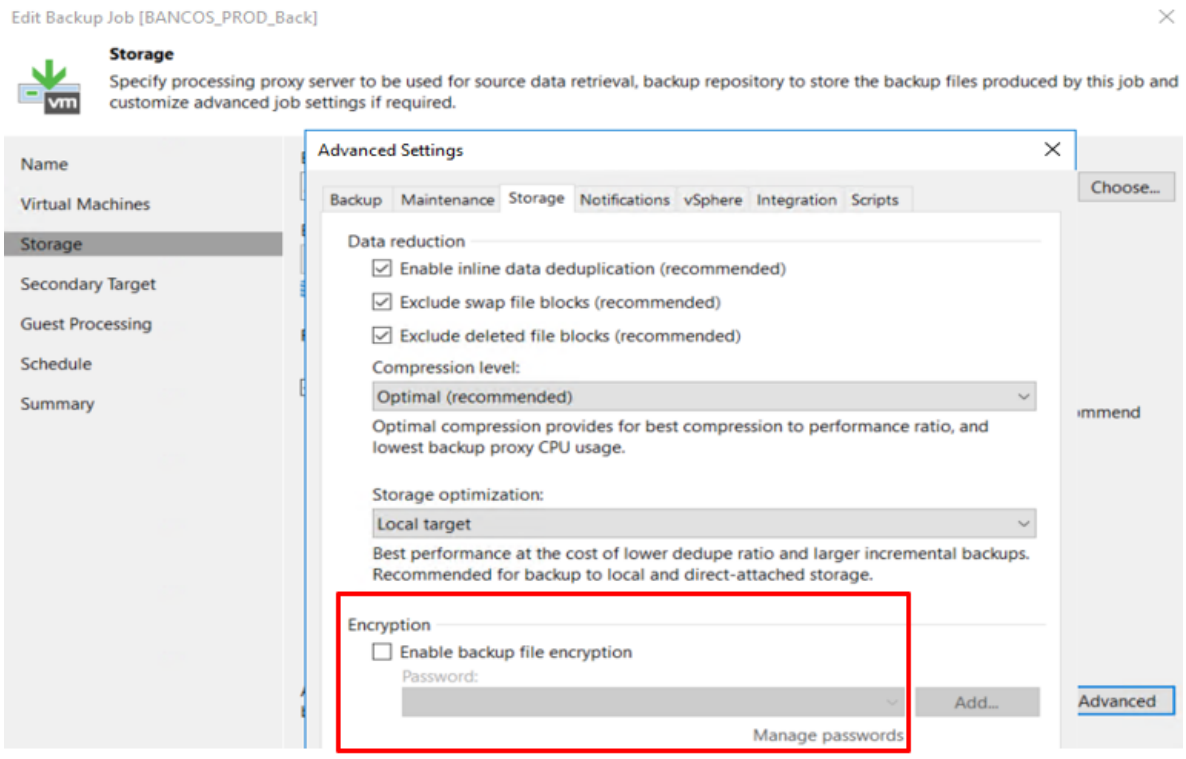


Cifrado end to end

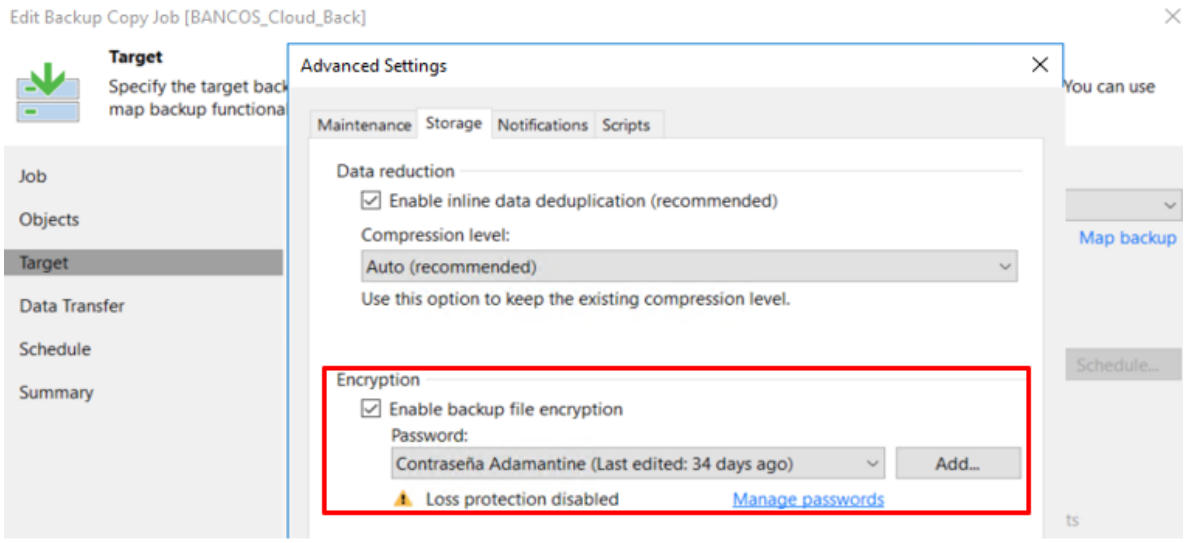
El cifrado del backup es fundamental en cualquier entorno de TI y no debería tener que adquirirse de forma independiente. Veeam ofrece cifrado AES 256-bit end-to-end integrado proporcionando la capacidad de cifrar los archivos:

- Durante un Backup, antes de que abandone la red de Adamantine.
- Durante la transferencia entre componentes.
- Mientras los datos están almacenados en los repositorios.

Para la operación Adamantine los Backup locales (disco y cinta) no tienen cifrado por contraseña para conseguir un respaldo más rápido y mejor rendimiento en caso de una restauración, pero los Backup en la nube se encuentran cifrados por contraseña desde el 24 de septiembre de 2019. En caso de un evento de restauración de una máquina(s) virtual, los responsables del área de sistemas TI en Adamantine deben ingresar la contraseña de forma remota para proceder con su restauración en la nube* de los ambientes.



Configuración de encriptado de respaldos locales



Configuración de encriptado de respaldos en la nube

Restauración en la nube

Veeam Backup & Replication ofrece diferentes tipos de restauración, sin embargo, en caso de una contingencia critica utilizaremos FULL VM RESTORE como método principal, en la cual se incrementa el tiempo de restauración, pero mejora el rendimiento de los sistemas una vez finalizada.

La razón por la cual se incrementa el tiempo de recuperación es porque el respaldo de la maquina(s) se transfiere completamente del repositorio al sistema de almacenamiento de la infraestructura virtual de VMware productivo con niveles de redundancia que garantizan la alta disponibilidad.

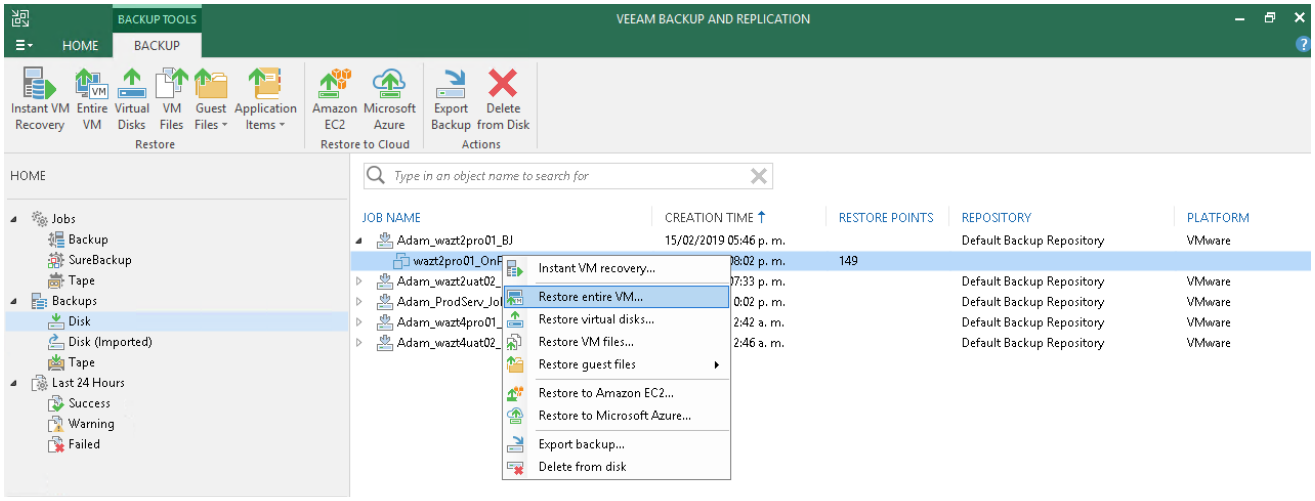
A continuación, listaremos los tipos de restauración que se pueden realizar desde el Repositorio en la nube de Veeam:

- **Full VM restore**
- VM files restore
- VM disks restore
- VM guest OS files restore
- Application items restore
- Disk export
- Guest OS files restore

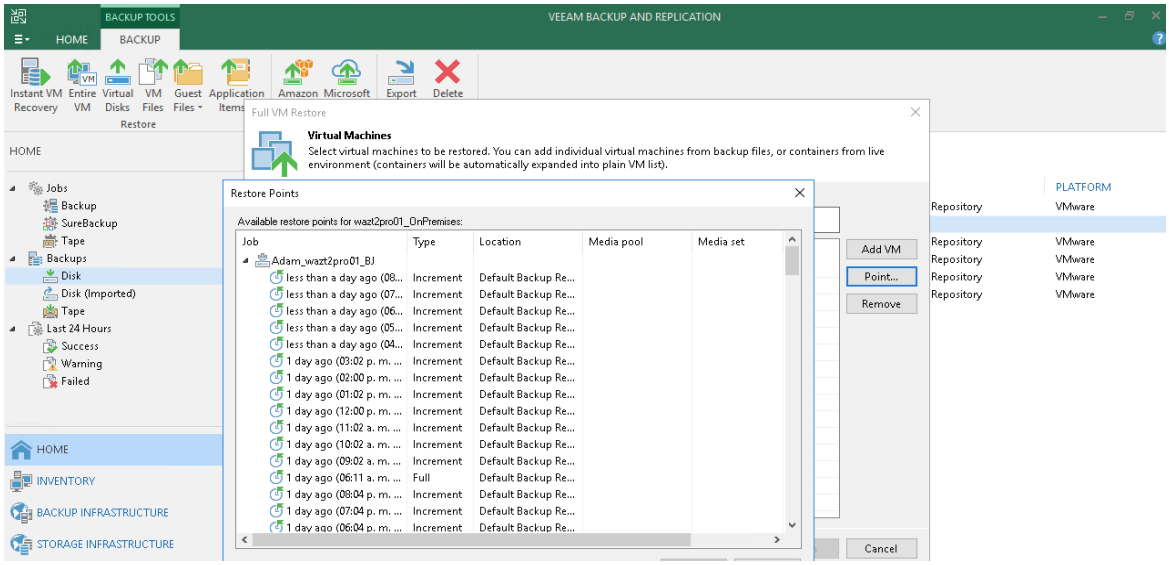
- Restauración completa desde repositorio (Disco)

Este método es aplicable cuando la máquina virtual no se puede restaurar localmente por problemas en el hardware, problemas de red, acceso al edificio o ante un posible desastre natural.

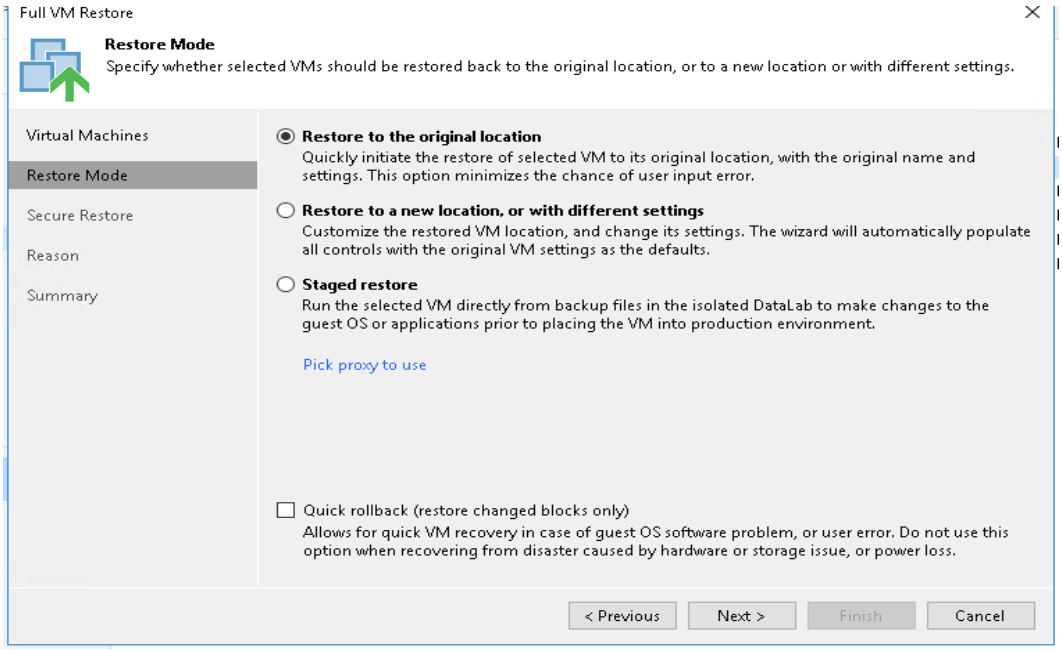
Para llevar a cabo este método nos dirigimos a la consola de administración de respaldos en la nube y seleccionamos el respaldo que deseamos restaurar, una vez hecho esto seleccionamos con el botón derecho “Restore entire VM”.



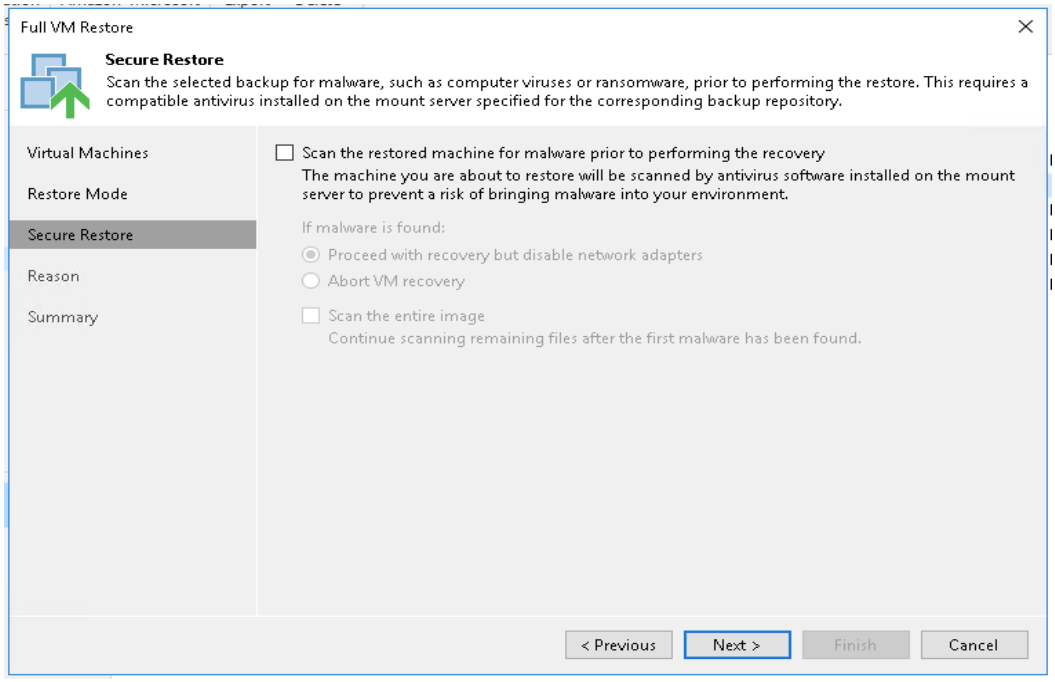
Dando un click en “Point” podemos seleccionar el punto de restauración en el tiempo de donde queremos restaurar la máquina.



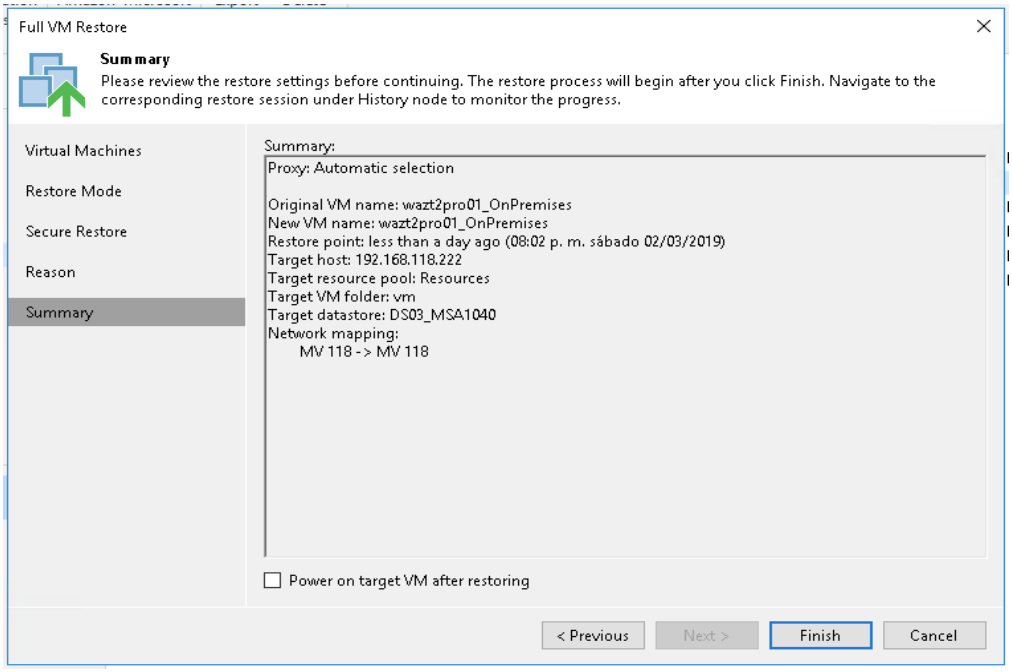
Seleccionamos el modo de restauración “Restore to a new location, or with different settings”, debido a que el respaldo original proviene de un repositorio diferente al Cloud repository.



Podemos realizar también el escaneo de la maquina por amenazas con un antivirus compatible



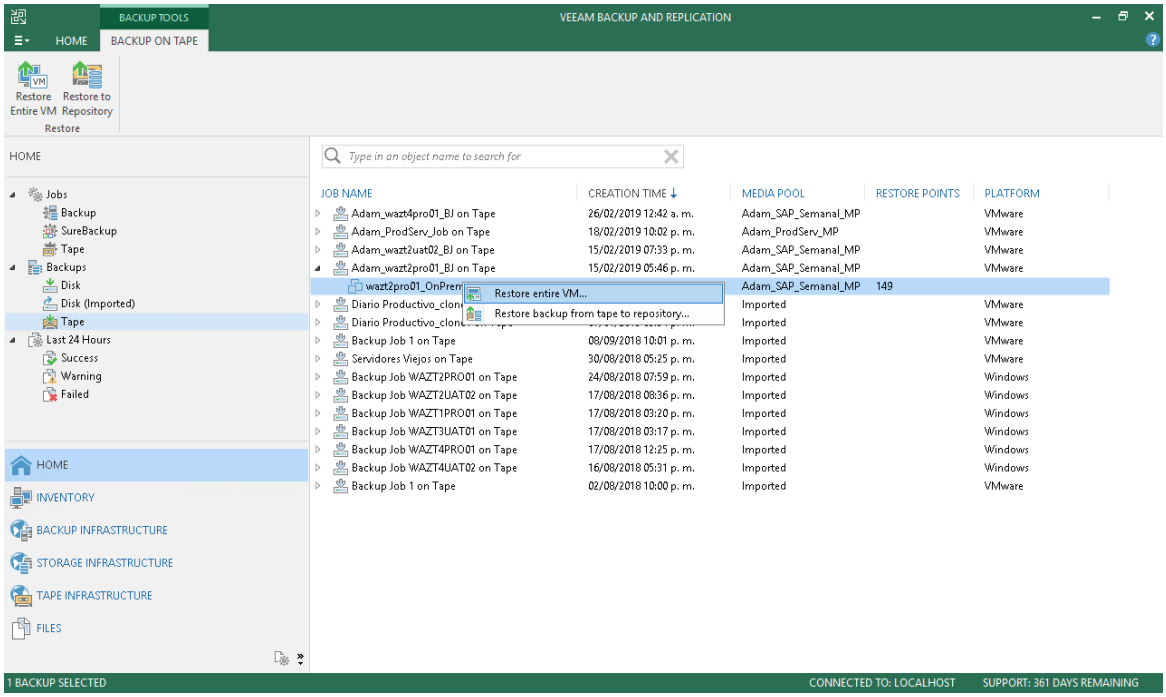
Una vez revisado el resumen de la restauración podemos dar clic en “Finish” y el proceso comenzará, el cual como ya hemos dicho antes requerirá el tiempo que el respaldo tarde en moverse por la red al DataStore de Producción.



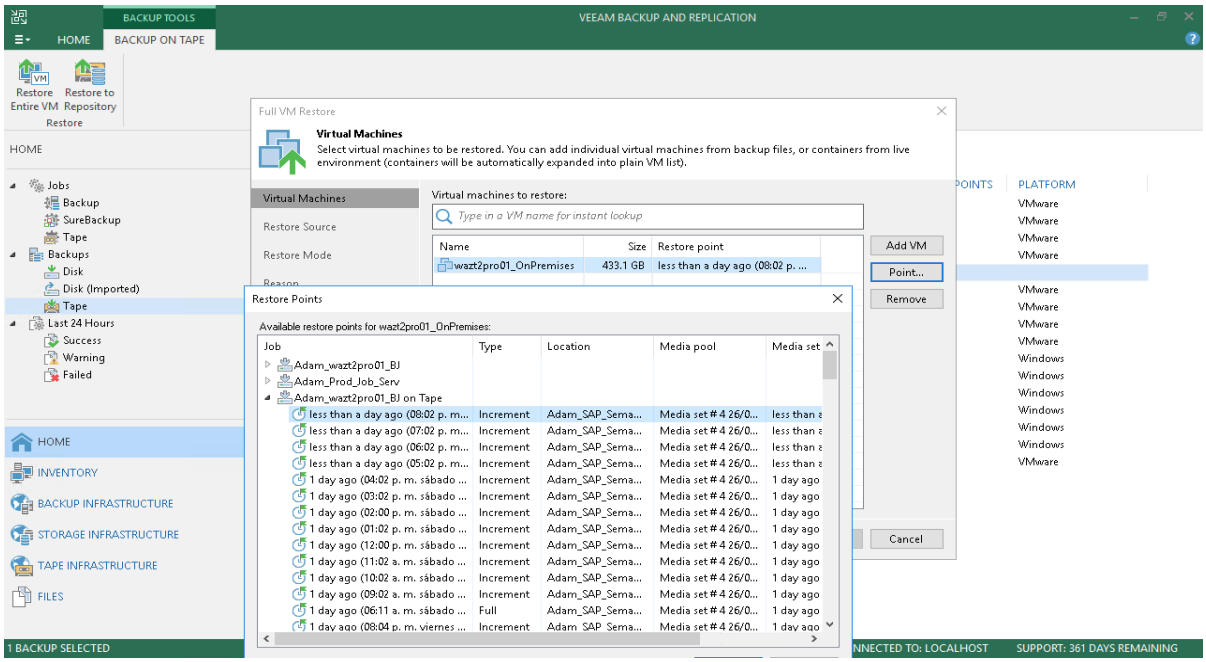
- Restauración completa desde Cinta

Como alternativa de restauración crítica, los respaldos almacenados en el repositorio en la nube se copian en un pool de cintas con un periodo de retención de dos semanas. La restauración de VM desde una cinta se ejecuta desde el menú “Tape” en el cual seleccionamos del lado derecho el respaldo especifico que queremos y damos clic con el botón derecho para desplegar el submenú donde usaremos la opción “Restore entire VM”

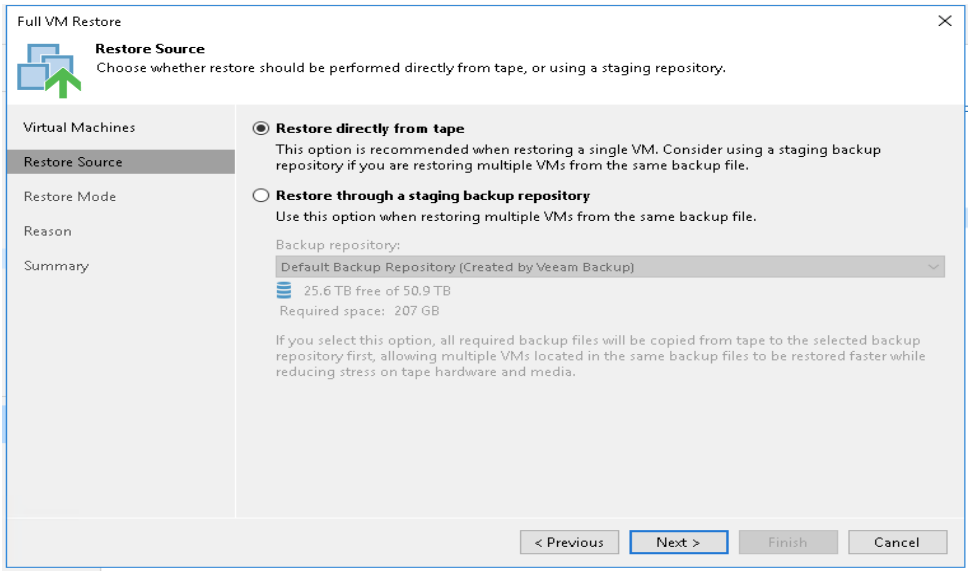
Esta opción restaura directamente desde la cinta. Si la cinta se encuentra en la librería, la restauración se realiza sin necesidad de pasar el archivo de respaldo al Repositorio (similar a restauración desde repositorio), por lo cual tendremos acceso a la maquina una vez que la restauración haya finalizado. En caso de que la cinta ya no se encuentre dentro, es necesario ingresarla y copiar el archivo de respaldo al repositorio. Posteriormente, se debe realizar una restauración desde el disco utilizando el archivo de respaldo copiado previamente.



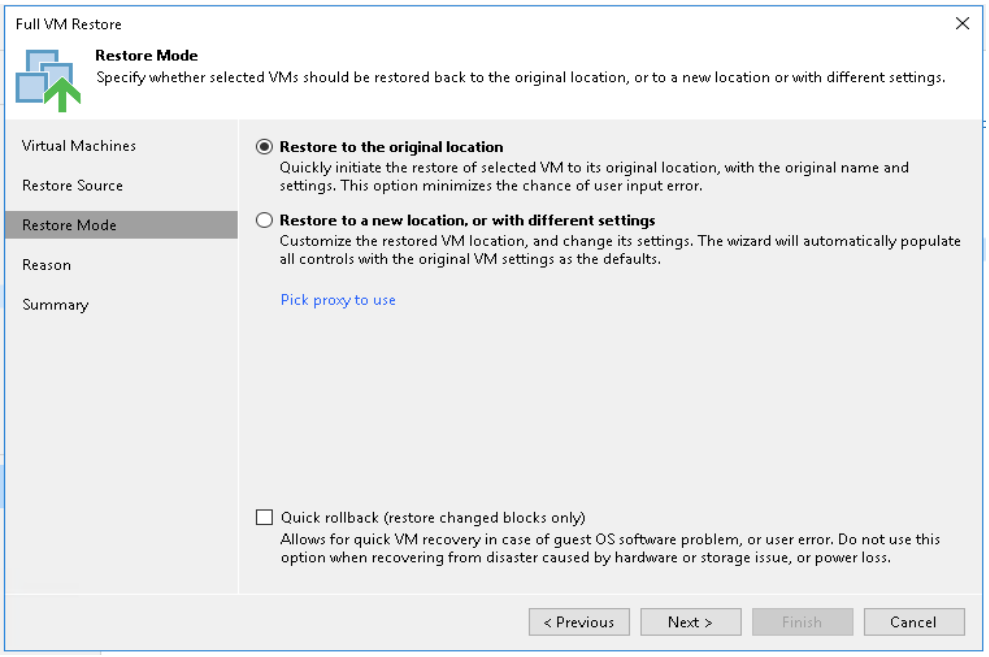
Seleccionando la opción “Point” tendremos acceso a todos los puntos de restauración en el tiempo, bajo el apartado “On Tape” como se muestra a continuación



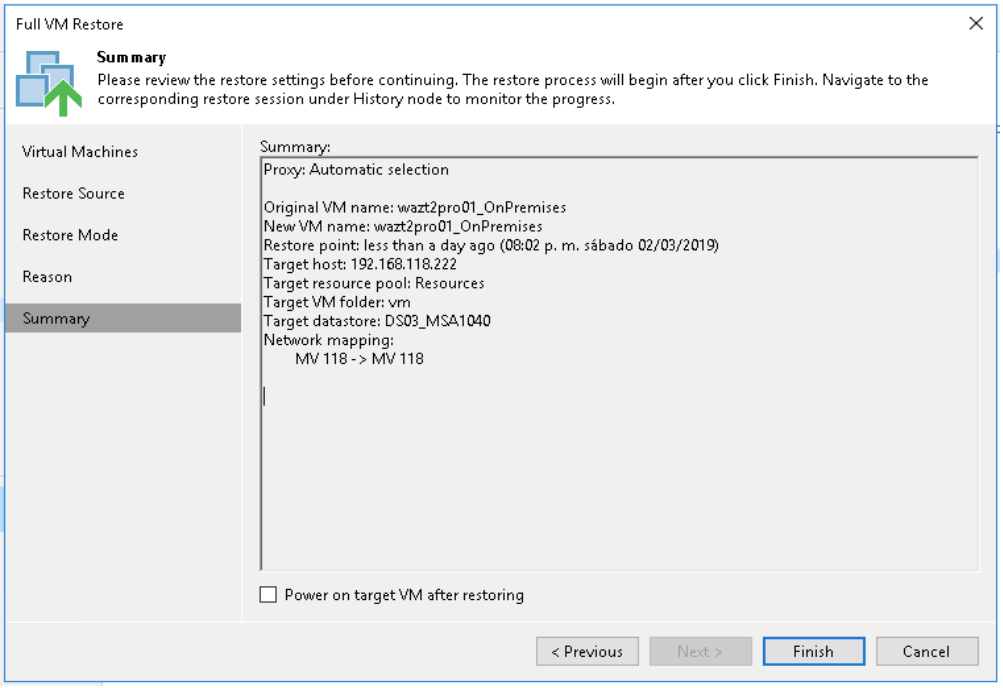
Al restaurar directamente de cinta, esta se ocupa por completo y no es posible realizar otras restauraciones de esta, por lo tanto, si se requiere restaurar varias máquinas al mismo tiempo, usaremos la opción “Restore trough a staging backup repository” y seleccionar el Repositorio donde se colocará el Backup, para este ejemplo usaremos el directo desde la cinta con la opción “Restore directly from tape”



En la siguiente ventana tendremos disponibles las opciones que ya hemos revisado antes como lo son restaurar a la ubicación original, a una ubicación diferente y hacer un “Quick Rollback” según sea necesario.



Por último, solo basta con dar clic a “Finish” para que el proceso se lleve a cabo.



Una vez que las máquinas virtuales que integran los ambientes productivos han sido restauradas se tienen dos puntos críticos para la continuidad del negocio:

1. Validación de los procesos, servicios y aplicaciones en los servidores
2. Acceso a las aplicaciones para los usuarios

Instalaciones de Sitio Alterno para Continuidad de Negocio

Sitio Alterno

- Requisitos para las instalaciones del DR alterno

Instalaciones propias diseñadas y construidas para continuidad de negocio, con ubicación y fácil acceso en la Ciudad de México, disponibilidad y servicios de seguridad 7 x 24, sistema redundante de producción de energía, estacionamiento y seguridad perimetral.

- Posiciones alternas de trabajo.

Lugares de trabajo para personal clave en caso de contingencia. Cómputo, telefonía e Internet con disponibilidad 7 x 24.

- Servicios adicionales

Sala de juntas, laptop, lockers para resguardo de pertenencias, servicio de impresión, espacio para equipos de telecomunicaciones conectividad segura pública y privada.

Acceso Remoto

Localización de empleados de Adamantine

- Usuarios que estarán en sitio Alterno del DRP

Los usuarios que son convocados para sitio alterno, es el personal crítico de la empresa que ejecuta procesos los cuales influyen en decisiones y ejecuciones críticas, estarán físicamente en las reuniones y ejecuciones para restaurar la operación de la empresa.

Usuario	Sistema
CONTABLIDAD	SAP FI y BO
CONTABLIDAD	SAP FI
CONTABLIDAD	SAP FI
CONTABLIDAD	SAP FI
CONTABLIDAD	SAP FI y TAIS
ADMINISTRACION MAESTRA	SACEJ
ADMINISTRACION PRIMARIA COB EXT JUD	SMART
COMERCIAL ADMINISTRACION PRIMARIA	TAIS
Analista de Contabilidad	TAIS
ADMINISTRACION DE CARTERAS ORIGINADAS	SAP BO
FISCAL	SAP BO
FISCAL	SAP FI, SAP BO

CREDITO Y RIESGO	SAP BO
CUENTAS POR PAGAR	SAP FI
TESORERIA	SAP FI
CUENTAS POR PAGAR	SAP FI
TESORERIA INTERNACIONAL	SAP FI
TESORERIA INTERNACIONAL	SAP FI
CUENTAS POR PAGAR	SAP FI

- Usuarios que no fueron convocados a un sitio alterno del DRP

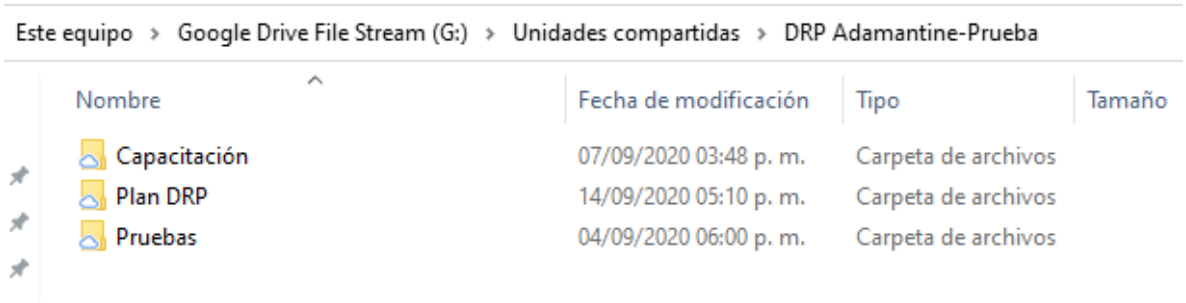
Tendrán que conectarse remotamente desde su localización después del desastre, por medio de una VPN o Citrix, las instrucciones serán enviadas a sus correos electrónicos. Todos los usuarios pueden conectarse a su correo electrónico desde cualquier máquina que cuente con internet y cualquier browser.

- Usuarios que estarán en esperando instrucciones

Los usuarios que no tienen actividades críticas esperarán instrucciones para reubicarse donde se les requiera, estarán disponibles y revisando su correo electrónico para recibir instrucciones.

Referencias

Ruta compartida – DRP Adamantine Prueba



Firmas de responsables

Director General	Sub director de Recursos Humanos	Sub director de Sistemas
Lic. Sergio Carrera Dávila Firma	Lic. Luis Felipe Flores Sánchez Firma	Ing. Juan Francisco Torres Sánchez Firma
Auditoría Interna	**Gerente de infraestructura**	**Líder del Proyecto- Analista de sistemas SAP**
Lic. José Luis Dávila Becerril Firma	Ing. Gerardo Enrique Butron Medina Firma	Ing Edith Paredes Ramírez Firma
Seguridad de la Información, Analista de infraestructura.	**Responsable Site Alterno**	
Ing. Víctor Manuel Agüeros Romero Firma		