Departamento de Informática

PROYECTO FIN DE CARRERA

Arquitectura, Implantación y Consideraciones de Seguridad en Plataformas Cloud. (Estudio en detalle de la Arquitectura de Cloud Computing con Ejemplos Prácticos).

Autor: Óscar Rivas Medina

Tutor: Miguel A. Ramos

Leganés, junio de 2015

Título: Arquitectura, Implantación y Consideraciones de Seguridad en Plataformas Cloud. (Estudio en detalle de la Arquitectura de Cloud Computing con Ejemplos Prácticos).
Autor: Óscar Rivas Medina.
Director: Miguel A. Ramos

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 23 de Junio de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Resumen

"Desde los albores de la civilización hasta 2003, la raza humana generó cinco exabytes de datos.
A día de hoy, producimos cinco exabytes cada pocos días, y el ritmo está acelerando"

Eric Schmidt – Director Ejecutivo – Google.

Los nuevos tiempos demandan nuevas infraestructuras, nuevas soluciones y nuevas ideas. Las infraestructuras de Tecnologías de la Información tradicionales no ofrecen la suficiente flexibilidad, escalabilidad y consolidación a sus usuarios, en un mercado que demanda de los proveedores de servicios y empresas cada vez mayor eficiencia.

Las infraestructuras de Computación en la Nube dan respuesta a estas demandas, ofreciendo a sus usuarios (particulares, organismos gubernamentales o empresas) servicios homogéneos, accesibles a través de sus conexiones de banda ancha.

A lo largo de este Proyecto de Fin de Carrera presentaremos las dos caras de estas tecnologías:

- Los **beneficios** que ofrece en cuestiones como son la transparencia administrativa y adaptabilidad a las necesidades puntuales de cada usuario, así como en precio de los servicios debido a una alta consolidación de los mismos.
- Los nuevos **retos** (seguridad, gobernanza, conformidad a legislación, etc…) que surgen de un tipo de infraestructura con arquitecturas, formas de acceso y gestión muy diferentes a las tradicionales.

Finalmente presentaremos un ejemplo práctico de Desarrollo de Servicio, Arquitectura e Implantación de un **Servicio de Respaldo en la Nube** *ficticio*, que ofrece a sus usuarios la externalización de su infraestructura de Respaldo en infraestructura del Proveedor de Servicios, mediante la salvaguarda de su información vía red en dicha plataforma remota.

Palabras clave: computación, nube, seguridad, gobernanza, riesgo, conformidad, proveedor, servicios, virtualización, plataforma, CPD.

Abstract

"There was 5 exabytes of information created between the dawn of civilization through 2003. But that much information is now created every few days, and the pace is increasing"

Eric Schmidt – CEO – Google.

New times require new forms of infrastructure, new solutions and new ideas. Traditional Information Technology Infrastructures do not offer enough flexibility, scalability and consolidation to its users, in a market that demands increasing efficiency from service providers and companies.

Cloud Computing Infrastructures answer these demands, offering their users (individuals, companies or government agencies) homogeneous services accessible via broadband connections.

Throughout this thesis we introduce the 2 faces of these technologies:

- The **benefits**, such as administrative transparency and adaptability to the needs of each user, as well as in price of services due to high consolidation thereof.
- The new **challenges** (security, governance, compliance, etc...) that arise from a type of infrastructure with architectures, management and access methods that differ a lot from the traditional ones.

Finally, we will present a practical example of Service Development, Architecture and Implementation of a fictional **Cloud Backup Service**, which offers its users the outsourcing of their Backup infrastructure into the Service Provider one, by safeguarding their information via network in said remote platform.

Keywords: computation, cloud, security, governance, risk, compliance, provider, services, virtualization, platform, DC.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

1.1 Introducción y objetivos

Para sentar las bases de este Proyecto de Fin de Carrera, empezaremos por usar un resumen de la definición de Nube del NIST (National Institute of Standards and Technology)[1]:

"La Computación en Nube es un modelo que habilita un acceso por red ubicuo, cómodo y bajo demanda a un conjunto compartido de recursos computacionales (por ejemplo redes, servidores, almacenamiento, aplicaciones y servicios), los cuales pueden ser rápidamente provisionados y liberados con un mínimo esfuerzo de gestión o interacción con los proveedores de los mismos."

El principal objetivo de este Proyecto de Fin de Carrera es presentar, mediante la implantación de un ejemplo ficticio de servicio en una organización, los aspectos que separan las arquitecturas tradicionales de Segunda Plataforma de las nuevas infraestructuras de Computación en Nube, considerando los aspectos específicos de seguridad, implantación y operación de las mismas. También pondremos foco en establecer un marco de documentación de proyecto de estas soluciones, intentando establecer una línea base, tanto a nivel de prestador de los servicios, como de consumidor de los mismos.

[1] The NIST Definition of Cloud Computing

1.2 Estructura de la memoria

Para facilitar la lectura de la memoria, se incluye a continuación un breve resumen de cada capítulo:

- **Computación en Nube – Introducción** : En este capítulo se comenzará a establecer las principales características y componentes de las infraestructuras de Computación en nube, específicamente los siguientes puntos:
  - Características esenciales.
  - Modelos de Servicio.
  - Modelos de despliegue o implantación.
- **Transformación organizativa a la Nube** – Breve explicación de los pasos que debe dar una organización para pasar de una infraestructura tradicional a una en la Nube.
- **Migración de Aplicaciones a Infraestructuras de Computación en Nube** – Consideraciones específicas de la migración de aplicaciones a entornos en la Nube.
- **Gobernanza, Riesgo y Conformidad en las Infraestructuras de Computación en Nube** - Consideraciones de seguridad de carácter general aplicados a infraestructuras de Computación en Nube:
  - Principales Amenazas de Seguridad
  - Gobernanza Organizativa
  - Valoración de Riesgos.
  - Conformidad.
  - Privacidad.
  - Análisis Forense.
  - Marcos de Trabajo y Estándares.
- **Proveedores de Computación en Nube. Transitividad del riesgo** – Análisis acerca de los riesgos asociados a los Proveedores de Servicios en Nube y cómo afectan a las organizaciones que hacen uso de sus servicios.
- **Seguridad en elementos específicos de Infraestructuras en Nube** – En este apartado se expondrán brevemente consideraciones de seguridad de los principales componentes de una infraestructura de Computación en Nube:
  - Consideraciones de seguridad en entornos virtualizados.
  - Consideraciones de seguridad en sistemas de almacenamiento.
  - Consideraciones de seguridad en recursos de red.
  - Seguridad en redes de datos.
  - Seguridad en redes de almacenamiento.
- **Diseño de Arquitectura e Implantación del Servicio de Respaldo en la Nube** – Finalmente pasaremos a presentar la propuesta detallada de diseño e implantación del servicio de Respaldo en la Nube, aplicando todas las consideraciones expuestas anteriormente:
  - Definición Técnica del Servicio.
  - Definición Operacional del Servicio.
  - Manual Técnico del Servicio.

Capítulo 2

Introducción a la Computación en la Nube

2.1 Características esenciales

Se considera generalmente que las arquitecturas de Computación en la Nube poseen al menos las siguientes 5 características esenciales[2]:

- **Autoservicio bajo demanda** – Un consumidor de recursos puede, de manera unilateral, provisionar para su uso o el de otros, recursos de computación sin que sea requerida interacción con el proveedor de servicios.
- **Amplio acceso vía red** – Los recursos o capacidades de la infraestructura estarán disponibles a través de la red (Internet generalmente), y se accederá a los mismos a través de mecanismos estándar y dispositivos de toda índole.
- **Agrupación de Recursos *(Pooling)*** – Los recursos computacionales serán agrupados con el fin de ser útiles a varios consumidores, en un modelo de tenencia múltiple, con diferentes tipos de recursos tanto físicos como virtuales asignados de manera dinámica según las necesidades puntuales de cada momento. El consumidor de estos recursos, generalmente no tiene control o conocimiento sobre la localización exacta de los mismos, aunque, si fuese

[2] Essential characteristics of Cloud Computing

necesario, podría tomar control sobre ciertos aspectos a alto nivel (país, centro de datos, etc …)

- **Flexibilidad rápida** – Las capacidades de cada recurso pueden ser provisionadas y liberadas de manera elástica y, en ciertos casos, automática, con el fin de ajustarse a la demanda.
- **Servicio Medible** – Capacidad de monitorizar, controlar e informar de manera transparente tanto al proveedor como al cliente de la utilización del servicio, de cara a poder medir la calidad del servicio y optimizar el uso de recursos

Por tanto, una *infraestructura de Computación en la Nube* es el conjunto de hardware y software que permite ofrecer estas cinco características esenciales. Puede verse como el conjunto de 2 diferentes capas:

- **Capa física** – Consiste en los recursos de hardware que son necesarios para proporcionar los servicios de Computación en la Nube. Normalmente incluye servidores, almacenamiento y elementos de red.
- **Capa de abstracción** – Es el software que se implementa sobre la Capa Física y que hace usables las capacidades esenciales enumeradas con anterioridad.

2.2 Modelos de Servicios de Computación en la Nube.

Desde el punto de vista del tipo de servicio ofrecido al cliente por la infraestructura de Computación en la Nube nos encontramos con los siguientes Modelos de Servicio[3]:

- **Software como Servicio (*Software as a Service - SaaS*)** – Es la capacidad ofrecida al cliente de usar determinadas aplicaciones que se ejecutan en la infraestructura de Computación en la Nube. Estas aplicaciones deben ser accesibles desde cualquier tipo de dispositivo vía red. El consumidor no gestiona o controla la infraestructura de Computación en la Nube subyacente incluyendo red, servidores, sistemas operativos o almacenamiento.
- **Plataforma como Servicio (*Platform as a Service - PaaS*)** – Es la capacidad ofrecida al cliente de desplegar en la infraestructura de Computación en la Nube aplicaciones creadas por él mismo o compradas a otros, que estén soportadas por el proveedor del servicio. El cliente no controla ni gestiona la infraestructura de Computación en la Nube subyacente, al igual que en el caso de SaaS, pero tiene control total de la aplicación desplegada así como posiblemente de la configuración del entorno de la misma.
- **Infraestructura como Servicio (*Infraestructure as a Service - IaaS*)** – En este caso la capacidad ofrecida al cliente es la de provisionar capacidad de proceso, almacenamiento, redes y otros recursos computacionales fundamentales, en los cuales el cliente es capaz de desplegar y ejecutar software de manera arbitraria, lo cual puede

3 The NIST Definition of Cloud Computing

incluir sistemas operativos y aplicaciones. En esta modalidad, el consumidor tampoco controla ni gestiona la infraestructura de Nube subyacente, pero normalmente tendrá control sobre sistemas operativos, almacenamiento y las aplicaciones desplegadas, así como seguramente de determinados elementos de red.

2.3 Modelos de despliegue o implantación

- **Nube privada (*Private Cloud*)** – En esta tipología, la infraestructura de Computación en la Nube se despliega para el uso exclusivo de una única organización que comprende múltiples consumidores de recursos. Puede pertenecer, ser gestionada y operada por dicha organización, terceros o cualquier combinación de ambos, y su ubicación física puede ser tanto dentro como fuera de las instalaciones de la organización.
- **Nube Comunitaria (*Community Cloud*)** – La infraestructura de Computación en la Nube se provisiona para el uso exclusivo de una determinada comunidad de consumidores de recursos con preocupaciones similares acerca de seguridad, políticas, conformidad con estándares … Puede pertenecer, ser gestionada y operada por una o varias de las organizaciones, terceros o cualquier combinación de ambos, y su ubicación física puede ser tanto dentro como fuera de las instalaciones de las organizaciones que la conformen.
- **Nube Pública (*Public Cloud*)** – La infraestructura de Computación en la Nube se provisiona para el uso por parte del público en general. Está ubicada físicamente en las instalaciones de un determinado proveedor de servicios, que es quien los ofrece.
- **Nube Híbrida (*Hybrid Cloud*)** – La infraestructura de Computación en la Nube es una mezcla de dos o más infraestructuras en la Nube diferentes (Privada, Comunitaria o Pública) que mantienen identidades diferentes, pero que están unidas por una tecnología (propietaria o estándar) que permite portabilidad de datos y aplicaciones.

2.4 Conclusiones

La principal ventaja de las infraestructuras de Computación en la Nube frente a las tradicionales es la velocidad y agilidad que aportan a las organizaciones, así como los ahorros monetarios derivados de la reducción de recursos malgastados u obsoletos. Hay otra serie de beneficios, principalmente a nivel operacional, pero los principales beneficios son a nivel de negocio: Incremento en la **eficiencia** y **control cuantitativo** de los recursos.

A pesar de que los ahorros en costes que proporciona la Computación en la Nube a las organizaciones son muy importantes, el principal motor que impulsa a la tecnología

de Computación en la Nube es la **agilidad**, y suele ser el principal motivo que las lleva a invertir en este tipo de infraestructuras[4].

[4] Gartner Technology Research

Capítulo 3

Transformación organizativa a la nube

La evolución de las plataformas tecnológicas, desde las primeras nacidas durante los años 60 como medios de procesamiento de información centralizados (*mainframes*), a las siguientes y presentes hasta prácticamente nuestros días (segunda plataforma), y que cambiaron la naturaleza del procesado de información a otro menos centralizado y más distribuido, han llevado al nacimiento de la tercera plataforma.

Actualmente el acceso y procesamiento de la información se ve altamente influenciado por la aparición y adopción masiva de los dispositivos móviles, los cuales hacen accesible la información en tiempo real, por parte de prácticamente cualquier individuo.

Aún no hay un consenso acerca de la definición de la tercera plataforma, pero según el OpenGroup[5] las tecnologías en las que se apoya la tercera plataforma son principalmente:

- Computación móvil.
- Redes sociales.
- Computación en la Nube.
- Big Data

[5] The OpenGroup – Convergent Technologies Survey.

Debido a la naturaleza de la tercera plataforma, los *retos de seguridad* serán la principal preocupación de las organizaciones, tanto a nivel de confianza por parte de los usuarios, como a nivel de cumplimiento de legislación.

El proceso de transformación de una plataforma de segunda generación a una de tercera, comprende principalmente los siguientes pasos:

- **Paso de Físico a Virtual** – En esta primera fase, nos movemos de una plataforma con infraestructura dedicada y normalmente monolítica, a otra con recursos consolidados. Esto incluye virtualización de servidores, recursos de almacenamiento e integración de la administración de la plataforma. El resultado de la fase será una notable disminución de los requisitos de energía y espacio, así como un incremento de la productividad de los recursos de administración.
- **Operacionalización**[6] – El próximo paso parte de un entorno ya consolidado, y lo operacionaliza, es decir se explicitan todas y cada una de las variables que configurarán indicadores medibles que definan los servicios ofrecidos por la plataforma, como por ejemplo parámetros de seguridad, disponibilidad, rendimiento o requisitos de gobernanza. El resultado de la fase será una notable disminución de los gastos operativos y una mayor integración de la gestión, lo cual redunda notablemente en incrementar la seguridad de la plataforma, punto clave para medir el éxito de la implantación.
- **Transformación a Nube** – El último paso consiste en la transición a una infraestructura totalmente compartida y estratificada. Esto implica que los usuarios de la plataforma pueden desplegar su infraestructura en modo autoservicio dentro de los servicios ofrecidos por el catálogo.

Las infraestructuras de tercera plataforma serán las que usen las infraestructuras de Computación en la Nube, ya que sin ellas no es posible su despliegue en los términos mencionados anteriormente en el capítulo.

[6] Steps to Operationalize Private Cloud Computing

Capítulo 4

Migración de aplicaciones a infraestructuras de Computación en Nube

4.1 Proceso de Migración

El proceso de migración de aplicaciones a infraestructuras de Computación en la Nube presenta múltiples retos, ya que son complejas y dirigen el resto de decisiones a tomar durante el proceso de conversión a la Nube. Simultáneamente, la capa de aplicación es la que más tiene que ganar de una infraestructura de Computación en la Nube correctamente diseñada.

Usando tecnologías y técnicas disponibles en otras capas (física o de abstracción), el desarrollo de aplicaciones puede verse simplificado en gran medida, por ejemplo[7]:

- Varias aplicaciones heterogéneas pueden ser desplegadas y gestionadas de manera similar, gracias a las capacidades de orquestación y virtualización.

[7] Migrating Applications to Public Cloud Services: Roadmap to Success.

- Debido a las capacidades innatas de la infraestructura física sobre la que se apoyan, y las capacidades de los hipervisores, se puede incrementar drásticamente el tiempo de actividad de una aplicación sin gastar recursos de desarrollo en implementar dicha funcionalidad.
- Eliminación de complejidades innecesarias (planes de actualización masiva, silos, etc…).

El desarrollo de aplicaciones tradicionales ya es un reto en sí mismo, siendo los desarrolladores los responsables de mantener los estándares de seguridad como prioridad principal. En los entornos actuales, los usuarios pueden estar distribuidos a través de distintas sedes de una organización, o incluso distribuidos a lo largo y ancho del planeta usando dispositivos móviles. Todo indica que esta tendencia va a ir en aumento, y adicionalmente, la aplicación en sí misma también puede estar distribuida, con múltiples niveles de presentación.

Estas diferencias, generan nuevos retos y requerimientos de seguridad, tanto en las aplicaciones como en la infraestructura que las soporta. Asimismo, este factor de cambio ofrece una oportunidad de reevaluación de inventario en los Centros de Proceso de Datos tradicionales, ya sea físico, de aplicaciones o datos, aumentando de manera inherente la seguridad.[8]

De cara a integrar las aplicaciones de la organización en la Nube, hay que clasificarlas, así como los datos que manejan. Esta clasificación es vital, y será un factor de decisión a la hora de planificar la infraestructura que necesitará.

Los tipos de aplicaciones a considerar son los siguientes:

- **Aplicaciones Heredadas** – Una aplicación antigua, que sigue siendo usada por una determinada necesidad de la organización. Típicamente se ejecuta en hardware lento y quizá obsoleto.
  Este tipo de aplicaciones, generalmente, no se adaptan bien a una infraestructura en la Nube, y es necesaria una significativa cantidad de trabajo a la hora de ser integradas.
  Migrar la aplicación a un entorno más moderno puede resultar atractivo, pero muchos sistemas heredados están basados en plataformas propietarias no compatibles, y el coste de adaptación puede ser muy alto.
- **Aplicaciones Corporativas** – Se utilizan para resolver un problema global de la organización, y son usadas por la mayoría de la misma. En términos generales, se pueden definir como aplicaciones de misión crítica, y son necesarias para el correcto funcionamiento de la organización.
  Los típicos requerimientos de este tipo de aplicaciones son *clustering*, gran cantidad de recursos computacionales y alto ancho de banda.
- ***Big Data*** – Normalmente manejan grandes volúmenes de datos que tienen determinados atributos. Ejemplos habituales incluyen Redes Sociales, Minería de Datos (*Apache Hadoop Framework*) así como aplicaciones de adquisición y análisis de inteligencia de negocio.

[8] A Comparison of On-premise to Cloud Migration Approaches

Un típico error a la hora de catalogar las aplicaciones como Big Data es exigir un volumen de datos grande. No solo se busca esta característica, que muchas veces es cierta, sino también dificultad de procesamiento y la combinación de fuentes de datos tanto estructuradas como no estructuradas.
Aplicaciones consideradas como Big Data, se enfrentan a problemas de continuidad de negocio, retención de datos y seguridad propios, debido a los inusualmente grandes conjuntos de datos de los que suelen hacen uso.

- **Escala Web**– Software usado por un amplio grupo de usuarios (normalmente en el ámbito de los cientos de miles, o incluso millones). Ejemplos de estas aplicaciones podrían ser *Twitter* o *iTunes*.
  Los condicionantes de seguridad de este tipo de aplicaciones son especialmente importantes, ya que cualquier brecha puede afectar a muchos millones de usuarios.
- **Aplicaciones Móviles** – Generalmente se ejecutan en dispositivos de acceso alternativos, como pueden ser teléfonos móviles o tabletas. Debido a su naturaleza (acceso remoto a datos) suelen usar protocolos estándar de internet como HTML, RSS, XML etc.
  Suelen estar escritas para un determinado tipo de dispositivo o sistema operativo, y acceden a aplicaciones Web que residen en servidores remotos.

Hay que tener siempre en cuenta que las tecnologías usadas en una infraestructura de Computación en la Nube son dictadas por las aplicaciones que van a consumir los recursos, y éstas determinan la capacidad de procesamiento, memoria, almacenamiento y ancho de banda que serán necesarios para cumplir con sus requerimientos.

Estos requerimientos de recursos, deben permitir a las aplicaciones ejecutarse con respecto a unos estándares ya definidos anteriormente durante la fase de *Operacionalización*, así como escalar, es decir, incrementar su capacidad de manejar más datos, más clientes o una zona geográfica mayor.

4.2 Consideraciones de continuidad de negocio y tolerancia a fallos.

Las aplicaciones fallan. En mayor o menor medida, con mayor o menor regularidad, pero el diseño de una infraestructura en la Nube tiene que basarse en esta asunción.

La aplicación en sí, debe ser construida con la Tolerancia a Fallos en mente, es decir, cada elemento que la compone no debe ser totalmente dependiente de cualquier otra parte que falle.

Esto también aplica para aplicaciones distribuidas, es decir, el fallo de cualquier nodo de un clúster o segmento individual no debe interrumpir o parar completamente la aplicación en su conjunto.

También habría que tener en cuenta a la hora de diseñar una aplicación la persistencia de sus datos, es decir, que sean almacenados en medios de almacenamiento persistente, asegurar la existencia de copias de respaldo y de réplicas remotas, para cubrir el caso en que haya que recuperarse de un desastre.

Ya se esté usando una Nube Pública o Privada, el diseño de un plan de Continuidad de Negocio para las aplicaciones es vital. Desde el punto de vista del diseño, debemos tener en cuenta que los usuarios esperarán al menos el mismo nivel de disponibilidad y continuidad de negocio ofrecido por sus Centros de Proceso de Datos tradicionales, por lo que de antemano hay que obtener los siguientes datos del proveedor de servicios de Computación en la Nube (ya sea interno a la organización o externo):

- Detalles acerca del plan de Continuidad de Negocio para las Aplicaciones e Infraestructura.
- Explicación detallada del proceso de Respaldo de los datos, incluyendo valores para Punto Objetivo de Recuperación y Tiempo Objetivo de Recuperación.
- En caso de catástrofe que cause indisponibilidad del servicio ¿cuánto tiempo tardarían en volver a estar operativos los sistemas?

Se pueden encontrar un modelo de lista de comprobaciones en el Anexo 1 del presente documento. Su finalidad sería establecer una línea base de comprobaciones de índole general que aplicarían a cualquier tipo de organización. Esta lista puede usarse para valorar distintos proveedores, de cara a elegir a cuál de ellos migrar nuestra plataforma o aplicación, y de esta forma, cuantificar y comprobar que cumplen los requisitos mínimos de nuestra organización.

Capítulo 5

Gobernanza, Riesgo y Conformidad (GRC) en las Infraestructuras de Computación en la Nube

5.1 Introducción

En este capítulo nos centraremos en las consideraciones de Gobernanza, Riesgo y Conformidad que afectan a las infraestructuras de Computación en la Nube, y como afectan en su planificación y diseño.

El proceso de Gobernanza, Riesgo y Conformidad es una aproximación a nivel global dentro de una organización que asegura el funcionamiento correcto de la misma de acuerdo a sus políticas internas, regulaciones externas y condicionantes éticos.

Existe, a nivel general, un cierto grado de preocupación acerca de las implicaciones de usar infraestructuras de Computación en la Nube[9]. Los Gobiernos de

[9] Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model

todo el mundo están con su mirada fija en la Nube y considerando la introducción de nuevos controles regulatorios.

Un estudio de investigación de las pérdidas debidas a varias brechas en la seguridad informática de la compañía TJX[10] (una gran cadena de supermercados estadounidense), muestra que los costes asociados para la compañía superaron los mil millones de dólares en gastos orientados a mitigar sus efectos. Alrededor de dos tercios de dicha cantidad fue debida a pérdida en valor de acciones, costas procesales, multas y consultoría; los costes de daños y perjuicios en sí fueron el tercio restante.

Otro ejemplo clásico de brecha de seguridad es el caso de Heartland[11], que ha costado a la compañía alrededor de 250 millones de dólares en concepto de gastos judiciales y daños y perjuicios.

Lo que lleva a una organización a tener un programa de Gobernanza, Riesgo y Conformidad suelen ser motivos externos, como por ejemplo:

- Una violación de seguridad que causa pérdida de información y que, debido a las regulaciones, genera denuncias.
- Creación de nuevas legislaciones que afectan a la organización.

Es decir, en muchas ocasiones, las organizaciones aceptan el riesgo que supone estar expuestas a brechas de seguridad, hasta que, finalmente, sufren una.

Los principios clave de la seguridad son **confidencialidad, integridad y disponibilidad**. Estos principios han de relacionarse directamente con las estrategias de Gobernanza, Riesgo y Conformidad y el concepto de Computación en la Nube, haciendo énfasis en lo siguiente:

- Es necesario que la organización tenga la propiedad de la información, sin importar quien la almacene o la mantenga.
- Preparación de la información de la organización para la Nube. Hay que entender claramente los siguientes puntos:
    - Tipo de datos que se van a almacenar en la Nube.
    - Regulaciones y legislación que rigen sobre esos datos.
    - Escenarios y consecuencias de brechas de seguridad que afecten a datos almacenados en la Nube.
- Tener siempre un plan de acción sobre los datos, desde su creación hasta su borrado. Determinar los controles de seguridad que se vayan a necesitar para asegurar los correctos niveles de protección (por ejemplo cifrado). Este punto es **clave** ya que la mayoría de los datos afectados por regulación tienen requerimientos de ciclo de vida.
- Abordar la protección de los datos desde un enfoque multicapa, con defensa en profundidad, contrastación contra el modelo de confidencialidad, integridad y disponibilidad, y segregación de roles.

[10] The TJX Data loss and security breach case
[11] Lessons from the Data Breach at Heartland

Para realizar una transición segura a la Nube, las organizaciones tienen que mirar a los proveedores como una extensión de sus Centros de Proceso de Datos tradicionales, lo cual significa que la seguridad y los controles de Gobernanza, Riesgo y Conformidad deberían estar ya implantados, y ser de obligado cumplimiento con resultados medibles. El paso a la Nube no debería disminuir la exigencia de mejores prácticas de las empresas, sino más bien todo lo contrario.

5.2 Principales amenazas de Seguridad

Según datos proporcionados por la Cloud Security Alliance (CSA)[12] y la European Network and Information Security Agency (ENISA)[13], están son las principales amenazas de seguridad con las que deben lidiar las infraestructuras en la Nube:

CSA cloud security alliance	enisa European Network and Information Security Agency
• Abuso y uso incompetente de la Computación en la Nube • Interfaces y APIs inseguras. • Uso malicioso de información privilegiada. • Problemas con tecnología compartida. • Pérdida o fuga de datos. • Secuestro (*hijacking*) de cuentas de usuario o servicios.	• Perdida de gobernanza. • Bloqueo de proveedor (*Vendor Lock-In*) • Fallos de aislamiento. • Riesgos de Conformidad. • Protección de datos. • Borrado de datos inseguro o incompleto. • Uso malicioso de información privilegiada.

Tabla 1. Relación de principales amenazas de Seguridad en infraestructuras de Computación en la Nube

Vamos a entrar en detalle en los más relevantes desde el punto de vista de las políticas de Gobernanza, Riesgo y Conformidad:

- **Pérdida de Gobernanza** – En infraestructuras de Computación en la Nube, la organización cede el control de sus tecnologías de la información, y pasan a formar parte de un conjunto común de recursos, lo cual puede afectar a la seguridad. Los acuerdos de nivel de servicio (*SLAs*) con los proveedores pueden no comprometerse a facilitar determinadas medidas de seguridad como parte de este conjunto de recursos compartidos, dejando un vacío en los mecanismos de seguridad.
- **Bloqueo de Proveedor (Vendor Lock-In)** – En la actualidad, hay pocas herramientas, procedimientos, estándares o interfaces de servicio que garanticen la portabilidad de los datos, aplicaciones o servicios. Esto puede hacer que sea bastante difícil migrar de una infraestructura o proveedor a otro.

[12] Cloud Computing Top Threats in 2013.
[13] ENISA Threat Landscape 2014.

- **Fallos de Aislamiento** – En esta categoría se incluyen fallos de los mecanismos que separan recursos como por ejemplo almacenamiento, memoria, computación o redes entre diferentes usuarios de la infraestructura (por ejemplo, ataques de *guest hopping*[14]). No obstante, ha de tenerse en cuenta, que los ataques a los mecanismos de aislamiento (por ejemplo, contra supervisores de virtualización), son mucho menos numerosos y más difíciles de ejecutar que si los comparamos con los sistemas operativos tradicionales.
- **Riesgos de conformidad** - El dinero y tiempo invertido por una corporación en conseguir una determinada certificación (por ejemplo algún estándar de industria o algún requerimiento legal), puede ser puesto en peligro al migrar a una infraestructura en la Nube:
    - Si el proveedor de servicios en la Nube no puede aportar evidencias de que sus instalaciones están conformes a los mismos criterios y requerimientos que la infraestructura propia de la Corporación.
    - Si el proveedor no permite auditorías por parte del cliente.
    - En algunos casos, puede significar que en una infraestructura compartida, no se puedan conseguir ciertos niveles de conformidad (como por ejemplo la Ley Orgánica de Protección de Datos Personales).
- **Protección de datos** – Las infraestructuras en la Nubede Computación en la Nube pueden plantear riesgos para la protección de los datos de sus clientes. En algunos casos, puede ser difícil para un cliente de un proveedor de servicios en la Nube hacer comprobaciones efectivas acerca de cómo se manejan sus datos, y las prácticas que se utilizan para asegurar que se está actuando con ellos con respecto a los requerimientos legales.

- **Borrado de datos incompleto o inseguro** – Una petición de eliminación de un recurso de Computación en la Nube, puede no resultar en una auténtica limpieza de los datos. Puede darse el caso en el cual el borrado de los datos no sea posible exactamente cuándo desee el cliente, ya sea porque existen copias de los mismos que no están disponibles para su borrado o porque el almacenamiento subyacente que los alberga, también contiene datos de otro cliente o clientes. Esto obviamente aumenta el nivel de riesgo con respecto a la infraestructura dedicada.

[14] En este tipo de ataques, el atacante identificará dos máquinas virtuales que residen en el mismo nivel físico. Si asumimos que el atacante está interesado en datos que residen en la máquina A, pero no puede acceder a ella, intentará acceder a la máquina B, y después intentar acceder desde ella a la máquina A.

5.3 Gobernanza Organizativa

La Gobernanza a nivel Organizativo debe perseguir la distribución activa de los derechos de decisión, y las responsabilidades entre las distintas partes interesadas de la misma. Asimismo también debe fomentar la creación y aplicación de normas y procedimientos, de cara a poder monitorizar esas decisiones y de esta forma conseguir los comportamientos y resultados esperados.

En definitiva, un Sistema de Gobernanza IT Organizativo debe asegurar la efectividad, responsabilidad y la conformidad a las normas internas y legislación general.

Para que este sistema funcione, ha de distribuir la carga de trabajo y el proceso de toma de decisiones de manera eficiente e imparcial, además de definirse lo siguiente[15]:

- Quiénes van a dirigir, controlar y ejecutar las decisiones.
- Cuál va a ser el proceso de toma de decisiones.
- Qué información se requiere para poder tomarlas.
- Como se van a manejar las excepciones.
- Como se van a evaluar y mejorar los resultados del proceso de Gobernanza.

Este último paso es crítico, ya que cierra el ciclo, midiendo el resultado del proceso de Gobernanza, desvelando áreas de mejora e implantando los cambios propuestos de cara al futuro.

5.4 Valoración de Riesgos

Podemos definir el riesgo como el potencial de una acción o actividad (incluyendo el no realizar ninguna acción) de llevarnos a un resultado no deseado.

En las Infraestructuras en la Nube se deben valorar y tener en cuenta nuevos factores de riesgo, debido a su diferente naturaleza comparadas con los Centros de Proceso de Datos tradicionales. Estos nuevos factores podrían ser:

- Ahora que los datos o aplicaciones no se mantienen en un sistema dedicado y forman parte de un pool de recursos compartidos por varios usuarios, ¿cuáles son las implicaciones desde la perspectiva del análisis de riesgos?
- Al movernos a un entorno en la Nube, ¿tiene la infraestructura los controles adecuados para asegurar que los datos no crucen fronteras si esto no está permitido por las regulaciones o leyes locales?
- ¿Existen controles claros y exhaustivos hacia terceras partes (proveedores de nuestro Proveedor de Servicios), bien documentados, de cara a reducir el riesgo tanto como sea posible?

[15] Governing the Cloud.

- Si ocurre una incidencia, ¿hay una clara definición de dónde, cuándo y quién se encargará de ello para facilitar una respuesta eficiente a los escalados y análisis forenses?

Este proceso de evaluación del riesgo de cada Organización debe ser elaborado dentro de la misma, conociendo todos y cada uno de los factores, tanto externos como internos, que influyan en su creación. Los puntos básicos que debería contener todo proceso de evaluación de riesgo, y que pueden valer como plantilla para procesos de evaluación más complejos, son los siguientes[16]:

1. Ejecutar una comprobación de riesgos rápida y de alto nivel: En este paso utilizaremos simplemente una escala de riesgo y conformidad con los valores bajo/medio/alto/extremo.
   Si un determinado activo tiene un valor de alto o extremo quizá no sea un buen candidato para ser configurado en un entorno compartido, no obstante, el riesgo puede ser mitigado por controles más fuertes. Por ejemplo, si un recurso de información tiene que ver con Propiedad Intelectual, las políticas de la Organización pueden prohibir que salga de la misma, pero sin embargo, podría residir internamente en recursos compartidos donde se hayan instaurado controles lo suficientemente estrictos.
2. Basándonos en la calificación de riesgo, determinar qué medidas de mitigación tienen que aplicarse para poder migrar el recurso a un entorno en la Nube. Este proceso puede resultar muy complicado y caro (monetariamente y a nivel de recursos humanos). No obstante, este análisis puede mostrar cómo, con los estándares apropiados, y con nuevos y mejorados controles de seguridad, el recurso puede residir en infraestructura compartida.
3. Realizar un análisis de riesgos completo y en profundidad. Comprender y asimilar si se continúa expuesto a algún riesgo o problema de conformidad y aplicar medidas correctoras cuando sea necesario.
4. Desplegar el recurso en el entorno compartido. Los controles de seguridad deberían estar cumpliéndose correctamente, así como todos los requerimientos de conformidad.
5. Reevaluar el entorno con otro análisis, el cual podría incluso ser una auditoría externa.

Los enfoques primarios a la hora de la ejecutar la evaluación del riesgo, deben ser siempre los principios de la seguridad (confidencialidad, integridad y disponibilidad), pero ante todo, hay que tener en cuenta el valor de la aplicación y de sus datos para la Organización.

[16] Introducing Risk Management into Cloud Computing.

5.5 Conformidad

Podríamos llamar Conformidad al estado de acuerdo con respecto a una serie de directrices, especificaciones o legislaciones establecidas.

El proceso de evaluación sería muy similar al que se aplica en los riesgos, pero enfocándonos en el aspecto de Conformidad del recurso. Para ayudarnos en el proceso podríamos considerar los siguientes factores:

- **Estándares -** ISO/IEC 27017, PCI DSS, etc…
- **Mejores Prácticas** – Valorar la utilización de evaluaciones hechas por expertos como CSA o ENISA.
- **Evaluación de Privacidad previa al despliegue en el nuevo entorno**: Este proceso se debe basar en los requerimientos regulatorios, es decir, evaluar profundamente cómo las regulaciones existentes hacen que una determinada aplicación sea de alto riesgo.
- Si los datos son manejados por terceras partes, evaluarlas para detectar posibles **riesgos transitivos**.
- **Usar aplicaciones específicas de análisis de riesgos**, como *OCTAVE Allegro* o *PILAR (Magerit*). Estas aplicaciones están diseñadas para evaluar un determinado recurso de información y emplear métodos cuantitativos para su análisis.

Un ejemplo de Marco Regulatorio en España, sería el caso de las Administraciones Públicas, las cuales, además de la LOPD (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal), se verían obligadas a cumplir con el siguiente marco legal regulatorio a la hora de contratar sus servicios en la Nube[17]:

- Ley de Contratos del Sector Público. (RD Legislativo 3/2011, de 14 de noviembre).
- Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos y RD 1671/2009 que desarrolla parcialmente esta ley.
- El Esquema Nacional de Seguridad (ENS) y el Esquema Nacional de Interoperabilidad (ENI) (Reales Decretos 3/2010 y 4/2010, de 8 de enero).

[17] Administración Electrónica – Leyes y normas reguladoras de ámbito estatal.

5.5.1 Consideraciones de Privacidad

Dentro del ámbito de la Conformidad, nos encontramos con los requerimientos de privacidad de datos. Las leyes y regulaciones de privacidad suelen aplicarse normalmente a datos de carácter personal, como datos financieros de particulares o expedientes de salud. Estas leyes varían en gran medida en función de la jurisdicción.

Muchos países o regiones tienen leyes muy estrictas acerca de qué datos se recogen, cómo se notifica a las personas de que se han recogido y de cómo se van a usar, quién va a tener acceso a ellos, si se van a compartir, cómo se protegen, etc. España tiene leyes específicas a este respecto (Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)). La mayoría de los países no permiten que datos de carácter personal regulados crucen fronteras.

Existe una metodología, reconocida internacionalmente, llamada Privacidad por Diseño[18], la cual establece unas mejores prácticas a implantar en las Organizaciones para aumentar el grado de Conformidad (especialmente en materia de Privacidad).

Según sus creadores: "Privacidad por Diseño promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización."[19]

Promueve los siguientes 7 principios fundamentales:

1. Proactivo, no Reactivo; Preventivo no Correctivo – No depender de ningún elemento externo para alterar los datos una vez se han recogido y solo recoger los datos necesarios, reduciendo de esta forma la exposición a riesgos desde el principio.
2. Privacidad como la Configuración Predeterminada – No requerir por parte de los usuarios activar las medidas de seguridad, activarlas de manera predeterminada.
3. Privacidad Incrustada en el Diseño – Siempre hay que conocer la información que se recoge, a donde se dirige, donde termina almacenada, y cuanto tardaría en eliminarse.
4. Funcionalidad Total – Que la privacidad no sea considerada un obstáculo o un inconveniente en el diseño. Hacer que funcione correctamente la convertirá en un plus.
5. Seguridad Extremo-a-Extremo – Protección de Ciclo de Vida Completo – Solo mantener los datos que necesitemos y borrar los que ya no necesitemos.
6. Visibilidad y Transparencia – Siempre que sea posible ser transparente en tus políticas acerca de cómo los datos se van a usar y por quién.
7. Respeto por la Privacidad de los Usuarios.

[18] Privacy by Design – www.privacybydesign.ca
[19] Privacy by Design – Los 7 principios fundamentales.

5.6 Legislación y Análisis Forense en Infraestructuras de Computación en la Nube

Antes de entrar en detalle, tenemos que tener un conocimiento básico de cómo nos impacta la legislación vigente. La legislación a tener en cuenta en España será la siguiente[20] [21]:

- Ley de Enjuiciamiento Civil.
- Derechos Fundamentales:
    - Derecho a la seguridad jurídica y tutela judicial, la cual nos garantiza un proceso penal con garantías.
    - Derecho al secreto de las comunicaciones.
    - Derecho a la vida privada. En este derecho se incluye el derecho a la intimidad, una vida privada, derecho al honor y la propia imagen. Asimismo se incluye la limitación del uso de la informática para proteger la intimidad.
    - Derecho fundamental a la protección de datos. En el año 2000 en la sentencia 292/2000, el Tribunal Constitucional crea el derecho fundamental a la protección de datos como un derecho diferente al de intimidad.
- Ley de Protección de Datos de Carácter Personal – Se establecen 3 niveles:
    - Nivel básico:
        - Aplicable a todos los sistemas con datos personales en general.
    - Nivel medio:
        - Datos de comisión de infracciones administrativas o penales.
        - Datos de Hacienda pública.
        - Datos de servicios financieros.
        - Datos sobre solvencia patrimonial y crédito, y
        - Conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.
    - Nivel alto:
        - Datos sobre ideología.
        - Datos sobre religión.
        - Datos sobre creencias.
        - Datos sobre origen racial.
        - Datos sobre salud o vida sexual.
        - Datos recabados para fines policiales.
        - Datos sobre violencia de género.

  Estos niveles se aplican de manera acumulativa.

- Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico.
- Ley de conservación de datos relativos a las comunicaciones y redes públicas.

[20] Análisis Forense de sistemas informáticos.
[21] Guía para clientes que contraten servicios de Cloud Computing.

- Código Penal: El Código penal nos muestra las actitudes que se han tipificado como delito. El concepto de delito viene descrito en el artículo 10 del Código penal (Ley Orgánica 10/1995, de 23 de noviembre) (CP): "son delitos o faltas las acciones y omisiones dolosas o imprudentes penadas por la Ley." Por tanto, en este apartado comentaremos todas aquellas acciones que se pueden considerar como delitos telemáticos según la LO 10/1995 y varias modificaciones posteriores:
    - Corrupción de menores:
        - Exhibicionismo y provocación sexual
        - Prostitución (art. 187 y 189.1):
    - Apología del delito:
        - Concepto (art. 18.1, párrafo 2°).
        - Apología del genocidio (art. 608.2).
    - Delitos contra el honor (art. 211):
        - Calumnias (art. 205).
        - Injurias (art. 208).
    - Delitos contra la intimidad (art. 197):
    - Defraudación electrónica.
        - Estafa (art. 248.2)
    - Apropiación indebida (art. 252).
    - Uso ilegal de terminales (art. 256):
    - Daños a ficheros informáticos (art. 264.2):
    - Piratería informática:
    - Delitos documentales.
        - Falsedades documentales (del artículo 390 al 400).
        - Infidelidad en la custodia (del artículo 413 al 416).
    - Protección de la contraseña (art. 414.2).

En el pasado, la legislación requería normalmente una determinada carga de documentación probatoria en formato analógico mientras se procedía con el litigio. El procedimiento judicial típico requería del acusado la presentación de esta documentación, la cual era solicitada por el demandante.

Hoy en día, las leyes se extienden al mundo digital, y pueden incluir dentro de esta documentación elementos como, por ejemplo, cualquier comunicación de entrada o salida de un teléfono inteligente, tableta, o cualquier otro dispositivo de ocio doméstico. Los documentos en sí mismos pueden ser comunicaciones digitales o incluso fotografías tomadas con dispositivos digitales.

Dada esta nueva situación, en el ámbito de la Computación en la Nube habría que aclarar el procedimiento mediante el cual se recogen y almacenan estos datos, para que puedan ser utilizados en un potencial proceso jurídico. Hay que tener en cuenta también que muchas veces, si en un proceso jurídico se necesitan ciertos datos por alguna de las partes, estos pueden residir en sistemas compartidos, lo cual implica ciertas consideraciones adicionales a nivel de privacidad.

5.7 Programas Marco y Estándares

Con mucha frecuencia, las regulaciones y la legislación hacen referencia a Programas Marco de Gobernanza (GRC) que establecen las mejores prácticas a la hora de implementar los controles de seguridad, y para realizar el seguimiento del cumplimiento de las regulaciones. Estos Programas Marco, a su vez, hacen referencia a determinados estándares (FIPS, Common Criteria, ISO 27001) como una manera de establecer qué componentes o tecnologías pueden usarse para implementar un determinado tipo de control.[22]

Los Programas Marco de Gobernanza (GRC) suelen ser holísticos y completos. Generalmente abordan los procesos, pasando por las personas, productos, tecnologías, partners y proveedores.[23] El objetivo final de estos Programas Marco suele ser la conformidad con las regulaciones existentes para de esta manera minimizar el riesgo de pérdida de confidencialidad, integridad o disponibilidad de cualquier activo de información regulado. Ejemplos de estos Programas Marco serían:

- CobiT (Control Objectives for Information and related Technology).
- Val IT.
- ITIL v3.

Los estándares están diseñados para ayudar a crear un lenguaje común para la evaluación de la Gobernanza y de esta manera crear una plantilla de trabajo con la que crear un punto de inicio válido para su análisis. Las características habituales de los estándares son las siguientes:

- Normalmente comienzan como conjuntos de mejores prácticas, y posteriormente se aprueban como estándares por una autoridad de certificación (por ejemplo ISO/IEC).
- Evolucionan (si es que lo hacen) muy lentamente.
- Suelen tener un punto de vista global y muy generalizado para poder ser aplicables en diferentes contextos.
- Pueden ser dirigidos (o pertenecer) por determinados organismos o comunidades (Organismos gubernamentales, o grupos de empresas que operan en el mismo negocio).

[22] http://cloud-standards.org
[23] IT Value Delivery, Risk IT, CobiT, Val IT und ITIL.

5.8 GRC y Proveedores en la Nube. Transitividad del Riesgo.

Las reglas de transitividad del riesgo son muy importantes cuando se tiene que lidiar con Proveedores de Servicios en la Nube. Las razones se pueden resumir en 2 básicamente[24]:

1. **SLAs (*Service Level Agreement* – Acuerdos de nivel de Servicio)** – Establece, de manera contractual, entre cliente y proveedor la relación y expectativas entre ambos a nivel de servicio.
   Una determinada aplicación puede ser desglosada en las partes individuales que la componen y que por tanto componen el servicio. La transitividad implica que el SLA final medido de una aplicación no es la media de la de sus partes, sino el valor más bajo (el eslabón débil del servicio). Por ejemplo si tenemos una aplicación determinada con una disponibilidad de su computación del 99.95%, una disponibilidad de su servicio de almacenamiento de un 99.99%, y una disponibilidad de un 0% en su servicio de mensajería, el valor final de su disponibilidad será de un 0%, no de la media de todos sus componentes.
2. Hay que asegurarse que los Proveedores de Servicios en la Nube que usan terceros para llevar sus Servicios de Seguridad Informática, requieran de ellos los mismos controles de seguridad y seguimiento de Estándares que usa el Proveedor de Servicios.

Es extremadamente importante revisar las políticas de seguridad y las condiciones de servicio de los Proveedores de Servicios en la Nube (en términos económicos, garantías de calidad y especialmente que reúnan los requisitos legalmente establecidos), especialmente a sus políticas de recolección y retención de datos, con quién los comparten. Otros aspectos a tener en cuenta son los siguientes[25]:

- La aplicación de la ley no puede modificarse contractualmente.
- Tenemos que dar nuestra autorización explícita a la participación de terceras empresas, y conocer quiénes son.
- Hay que tener en cualquier momento ubicados los datos geográficamente (especialmente los regulados)
- Asegurarse de que se pueden recuperar los datos personales de los que la organización es responsable (portabilidad).
- Solicitar garantías por parte del Proveedor de Servicios en la Nube de que no se van a conservar los datos personales si se extingue el contrato.
- Garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO).
- Definición clara de responsabilidades - ¿Qué ocurre cuando hay algún problema y se ha de asignar un responsable? Definición de indemnizaciones.
- Respuesta a incidentes – En el eventual caso de un incidente (principalmente brecha de seguridad), el Proveedor de Servicios puede no querer hacerlo público,

[24] Trust mechanisms for cloud computing.
[25] A Case for the Accountable Cloud.

pero ¿qué ocurre si el incidente ha afectado a nuestra organización, y sin embargo, nosotros sí tenemos que hacerlo público? ¿Cómo funciona el proceso de escalado?

Capítulo 6

Diseño de Arquitectura e Implantación del Servicio de Respaldo en la Nube

6.1 Introducción

6.1.1 Objeto

Este documento contiene la información técnica del Servicio de Respaldo en la Nube.

El propósito de este documento es el de servir de referencia para las áreas tanto técnicas como comerciales de: Operaciones, Soporte a Ventas y Marketing. En este sentido, recoge tanto información general útil para todos los destinatarios del documento, como información específica destinada a satisfacer las necesidades de información de los diferentes grupos que puedan hacer uso de este manual.

Asimismo, se intenta presentar esta información como un ejemplo real de documentación de un proyecto comercial, y de qué información es necesario entregar tanto al cliente del proyecto (en este caso un Proveedor de Servicios en la nube ficticio), como también proveer de una plantilla o documentación inicial que será usada por los

clientes del servicio, así como por los administradores del mismo durante su vida en producción.

Los detalles técnicos de esta documentación han sido generados con respecto a los manuales de arquitectura, implantación y seguridad de los productos usados en la misma, usando información pública ofrecida por sus fabricantes.

6.1.2 Definiciones y siglas

HBA	Host Bus Adapter
WAN	Wide Area Network
CPD	Centro de Proceso de Datos
DPA	Data Protection Advisor
NTP	Network Time Protocol

6.2 Descripción Técnica del Servicio

6.2.1 Descripción general del servicio

El proveedor de Servicios en la Nube decide ofrecer dentro de su gama de servicios una solución de respaldo de datos remoto deduplicado en la nube y con capacidad de generación de informes avanzados. La tecnología utilizada para el servicio se basará en sistemas de almacenamiento capaces de prestar conectividad por protocolo IP y de deduplicar la información. Tras litigación pública, el Proveedor de Servicios en la Nube ha decidido proporcionar estos servicios basándose en los productos *EMC Avamar Data Store* como solución de respaldo de datos y *EMC Data Protection Advisor* que se desplegarán en las instalaciones de su CPD en Madrid.

El servicio se propone resolver los desafíos asociados al respaldo tradicional, habilitando un respaldo rápido, eficiente y recuperable a través de toda la empresa, desde los CPD locales hasta los CPD remotos, oficinas remotas, equipos de oficina y portátiles. El servicio utilizará la tecnología de almacenamiento con deduplicación de datos global para identificar los segmentos de datos redundantes en el origen, reduciendo el respaldo de datos en un factor de más de 300 (Antes de transferirlos a través de la red). Esto permite a los usuarios utilizar la infraestructura existente de WAN para hacer el respaldo y recuperación en caso de desastre de oficinas y CPDs remotos. Los datos serán cifrados al vuelo y en reposo para mayor seguridad, y la gestión centralizada hace posible la protección de cientos de oficinas remotas de manera fácil y eficiente.

EMC Data Protection Advisor es la solución elegida para realizar la gestión centralizada de todo el reporte, análisis y alertas del respaldo y la restauración dentro de una solución de gama Empresarial, la cual integra dentro de este sistema de reportes, la posibilidad de integrar cualquier elemento que esté presente en la arquitectura de respaldo (Librerías, Switches FibreChannel, Switches Ethernet, HBA´s, tarjetas ethernet, etc.).

Inicialmente el servicio será soportado por una cabina Avamar Datastore de 10 TB de capacidad ubicada en el CPD de Madrid. Además, se dispone de una máquina virtual alojada en la infraestructura de Virtualización como servidor y base de datos de Data Protection Advisor.

El diagrama de comunicaciones del servicio es el siguiente:

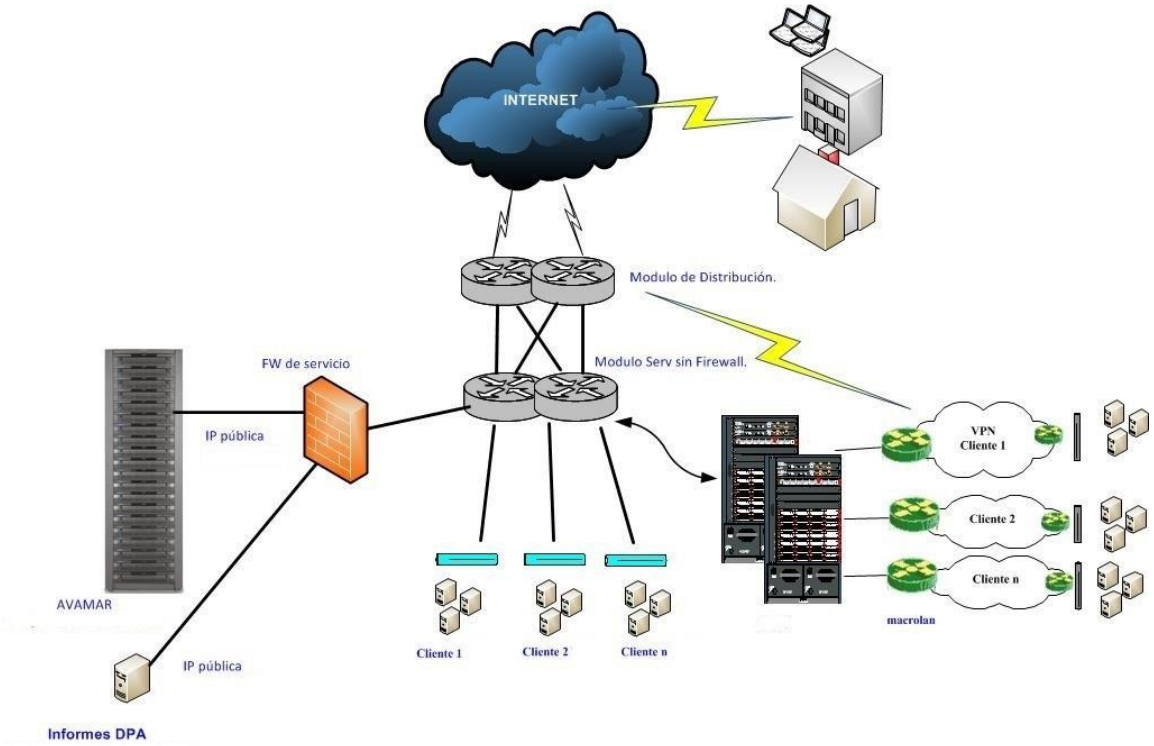


Figura 1. Diagrama de comunicaciones del servicio.

6.2.2 Deduplicación de Datos

Los datos empresariales son altamente redundantes, con archivos o datos idénticos guardados a lo largo de los diferentes sistemas (ej. archivos de SO o documentos enviados por correo a múltiples receptores). Los archivos editados también tienen una tremenda redundancia respecto de las versiones previas. El software tradicional de respaldo aumenta esta redundancia por el almacenamiento una y otra vez de todos estos datos repetidos.

El servicio utilizará su tecnología para la de-duplicación de datos y para mantener una sola instancia global de almacenamiento que elimina la redundancia a nivel tanto del archivo completo como de un segmento.

6.2.3 Software Cliente de Avamar

El servicio admite la protección automática de los sistemas operativos y aplicaciones líderes en el mercado. El cliente de Avamar filtra todos los datos repetidos antes de hacer el envío a través de las redes, haciendo posible la protección de sistemas en redes LAN o WAN colapsadas.

6.2.4 Componentes físicos

6.2.4.1 Nodo de utilidad

El primero de los componentes hardware del Servicio es un servidor de 2Us[26] que actuará como Nodo de Utilidad, encargado de programar y gestionar trabajos de respaldo y restauración. Provee servicios internos al sistema tales como consola de gestión, programación de tareas, autenticación externa, NTP y acceso web. El sistema operativo de este servidor es Red Hat Enterprise Linux. El Nodo de Utilidad no almacenará respaldos en ningún caso.

6.2.4.2 Nodo de Almacenamiento

Un Nodo de Almacenamiento es el que almacena la información de los respaldos. En el caso del servicio, se han instalado inicialmente tres nodos de almacenamiento con capacidad de 3.3TB cada uno que ejecutan el software de Avamar sobre Red Hat Enterprise Linux.S

Cada uno de ellos proporciona 5 conexiones GigaEthernet de cobre identificados como DRAC, eth0, eth1, eth2 y eth3. La conexión denominada DRAC provee acceso de consola al nodo, a través de la tecnología propietaria de Dell (Dell Remote Access Controller). El puerto eth0 forma un acoplamiento (*bonding)*[27] con eth2 y se conectan a un switch de servicio de sala del CPD de Madrid de forma que el nodo tiene alta disponibilidad de red para hacer tanto los respaldos como para comunicarse con el Nodo de Utilidad.

Además, cada Nodo de Almacenamiento dispone de fuente de alimentación redundante reemplazable en caliente.

6.2.4.3 Nodo de Almacenamiento de Repuesto

Se trata de un servidor de respaldo con las mismas características que un nodo de almacenamiento. Su estado habitual es inactivo a la espera de un fallo.

[26] Una unidad rack o simplemente U es una unidad de medida usada para describir la altura del equipamiento preparado para ser montado en un rack de 19 o 23 pulgadas de ancho. Una unidad rack equivale a 1,75 pulgadas (4,445 cm) de alto.

[27] Disposición en la cual dos o más interfaces de red se combinan a nivel lógico en uno, ya sea por razones de redundancia o de ancho de banda.

6.2.5 Componentes lógicos del Servicio

6.2.5.1 Agente Avamar

Un agente (o cliente) Avamar es una máquina que tiene acceso al servidor Avamar a través de una conexión de red.

El proveedor de Servicios proporcionará un nombre del dominio al cliente. El cliente utilizará ese nombre de dominio para activar sus máquinas.

Las tareas de instalación y actualización de agentes serán responsabilidad de los clientes del servicio, en ningún caso, serán funciones de los Grupos Técnicos del proveedor. Para ello, los clientes dispondrán tanto del manual de usuario del servicio como de la documentación técnica de producto y agentes disponibles a través del servidor web que publica la infraestructura del Servicio.

La lista de agentes soportados que se ofrece es muy amplia. La matriz de compatibilidad del siguiente enlace, muestra la lista de sistemas operativos y aplicaciones soportados:

https://community.emc.com/servlet/JiveServlet/previewBody/12543-102-1-47683/300-008-867.pdf

6.2.5.2 Dominio

Un dominio es una zona diferenciada dentro del servidor Avamar. Se utilizan para organizar los clientes y funcionan de forma jerárquica, pudiendo crear subdominios para facilitar una administración delegada.

Se configurará un dominio por cada cliente del servicio.

El nombre de dominio se codificará concatenando la fecha de provisión en formato americano codificada en hexadecimal, seguido del nombre del Cliente. Además, el nombre de dominio no debe superar los 20 caracteres.

Por ejemplo, el dominio interno del Proveedor de Servicios se dio de alta el día 7 de junio de 2015:

- 20150607 en hexadecimal: 133794F
- Concatenando el nombre: 133794FPS (PS → Proveedor de Servicios)

El Servicio sólo permite crear subdominios a usuarios *superadministradores* del sistema Avamar, con lo cual, si un cliente quiere utilizar subdominios, deberá solicitar al Proveedor de Servicios la creación de subdominios adicionales para dar distintos permisos administrativos.

Una vez creado el subdominio, el usuario administrador del dominio del cliente puede gestionar usuarios y clientes de su dominio y subdominios jerárquicamente.

En la Consola de Administración del Servicio, la estructura de dominios se muestra en muchas de las vistas disponibles, en el panel de la izquierda. El dominio *root* es siempre representado por el nombre del servidor de Avamar. Haciendo clic en el recuadro situado más a la izquierda de los dominios, se expande la estructura, mostrándose los subdominios y clientes que hayan sido asignados a dicho dominio. Hay varios dominios pre configurados por defecto, como son *MC_RETIRED* y *clients*. El dominio *clients* es el dominio por defecto y no puede contener ningún cliente del Servicio.

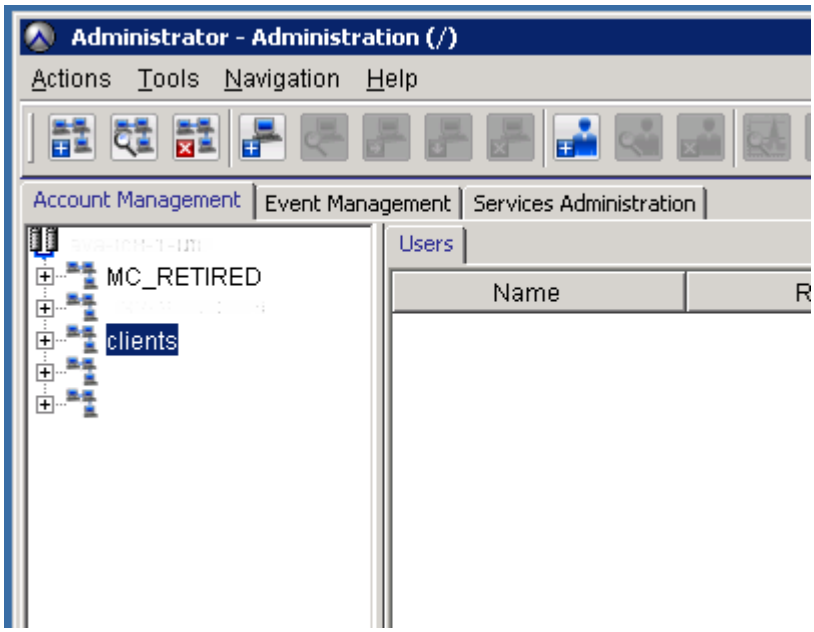


Figura 2. Administración de Dominios.

6.2.5.3 Activaciones

Para que un cliente pueda comenzar a hacer respaldos, es necesario que éste se active contra el servidor de Avamar. Para realizar la activación, el cliente debe conocer el nombre de dominio que el Proveedor de Servicios le haya asignado.

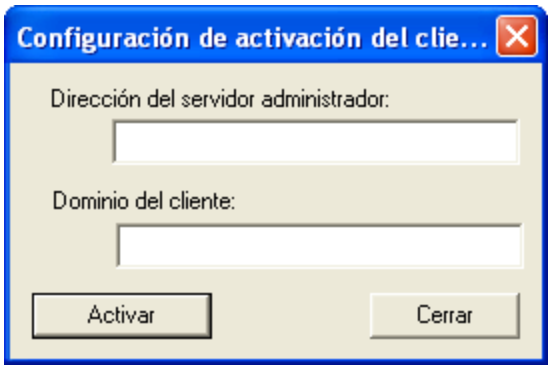


Figura 3. Diálogo de Activación del Cliente de Avamar.

6.2.5.4 Usuarios

Un usuario siempre tendrá asignado un rol, y el usuario siempre se creará dentro del dominio de un cliente.

Se creará una (y sólo una) cuenta de administrador de dominio Avamar por cada dominio de cliente. El cliente podrá crear cuentas de usuario adicionales sobre su dominio con diferentes roles (ver siguiente apartado).

Sólo se permitirá un usuario administrador del dominio de un cliente y éste se creará en tiempo de provisión de ese cliente.

El nombre de usuario administrador de un dominio siempre será "*admin*", independientemente del dominio.

El cliente podrá crear hasta un máximo de diez usuarios dentro de su dominio, con independencia de si tiene creados subdominios, es decir, la suma de los usuarios creados en el dominio padre de un cliente y sus subdominios no puede llegar a más de diez.

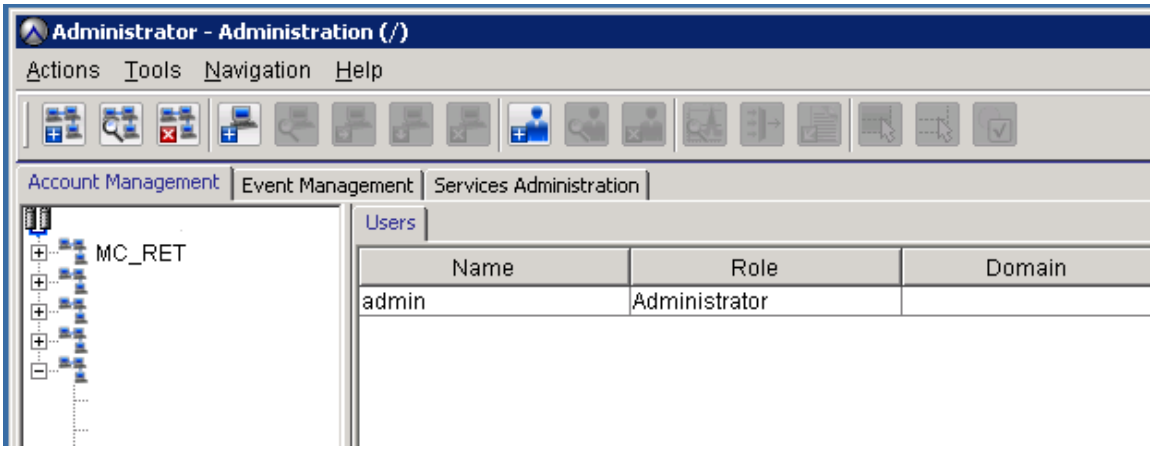


Figura 4. Vista de usuarios.

6.2.5.5 Roles

Los roles definen operaciones permitidas para cada cuenta de usuario. Hay dos categorías.

6.2.5.5.1 Administrador

Se creará una cuenta de usuario con rol de administrador dentro del dominio de cada cliente.

6.2.5.5.2 Operador

El rol de operador se da a ciertos usuarios para permitirles realizar respaldos y restauraciones de ciertas áreas del sistema.

El cliente podrá crear hasta un máximo de nueve usuarios con rol de operador dentro de su dominio.

Existen cuatro roles de operador:

- ***Restore only operator***: Sólo pueden realizar restauraciones y monitorizar esos trabajos de restauración. Si el rol se da al usuario en el dominio más alto, podrá realizar restauraciones de cualquier cliente. Si el rol se da al usuario en un dominio en concreto, podrá realizar restauraciones dentro de ese dominio.
- ***Backup only operator***: Sólo pueden realizar respaldos y monitorizar esos trabajos de respaldo (bajo demanda de cliente). Si el rol se da al usuario en el dominio más alto, podrá realizar respaldos de cualquier cliente. Si el rol se da al usuario en un dominio en concreto, podrá realizar respaldos dentro de ese dominio.
- ***Backup/restore operator***: Este rol es una combinación de los dos anteriores, es decir, los usuarios con este rol podrán hacer copias de respaldo, restauraciones y monitorizar como terminan esos trabajos.
- ***Activity operator***: Sólo permite monitorizar trabajos de respaldo y restauración a través de la consola de actividad y generar ciertos informes. Como siempre, dependiendo del nivel donde se asigne el permiso, se podrán monitorizar los trabajos a nivel global o a nivel de dominio particular.

6.2.5.6 Grupos y políticas de grupo

Una política de grupo es un objeto lógico que une los conceptos de conjunto de datos, calendario, política de retención y cliente. Los grupos se definen a nivel de dominio, y se pueden aplicar sólo a clientes de ese dominio. Una política de grupo controla el comportamiento de un respaldo a menos que se defina otro comportamiento a nivel de cliente.

Todo cliente debe pertenecer al menos a un grupo. El cliente se añadirá a un grupo como parte de la provisión inicial del mismo en el Servicio.

Dentro del dominio *root*, Avamar incluye un grupo pre configurado: el *Default Group*. Este grupo incluirá automáticamente todos los nuevos clientes siempre que ningún otro grupo sea configurado. El *Default Group* siempre utiliza el conjunto de datos, calendario y política de retención pre configurados. Esto no se puede modificar, sin embargo sí pueden modificarse las especificaciones del conjunto de datos, calendario y política de retención pre configuradas.

6.2.5.6.1 Conjunto de datos

Un conjunto de datos es un objeto que define el contenido del respaldo de un cliente. Es una lista de directorios y ficheros de los que se hará copia de respaldo. La ventaja que tienen es que es un objeto persistente aplicable a varios grupos o clientes.

Un conjunto de datos define:

- Lista de datos origen.
- Lista de exclusión e inclusión
- Opciones de complemento. Dependiendo del agente que haya instalado en el cliente habrá opciones adicionales para copias de respaldo referentes a bases de datos, sistemas de ficheros, etc.

Avamar provee cinco conjuntos de datos por defecto que se pueden utilizar como base para configurar los nuevos conjuntos de datos, cada uno de ellos adaptado a su entorno o sistema operativo: *Base dataset, Default dataset, Windows dataset, UNIX dataset, VMware dataset*.

El cliente podrá crear conjuntos de datos dentro de su dominio.

La recomendación es crear el menor número de conjuntos de datos posible ya que se complica la gestión para el cliente.

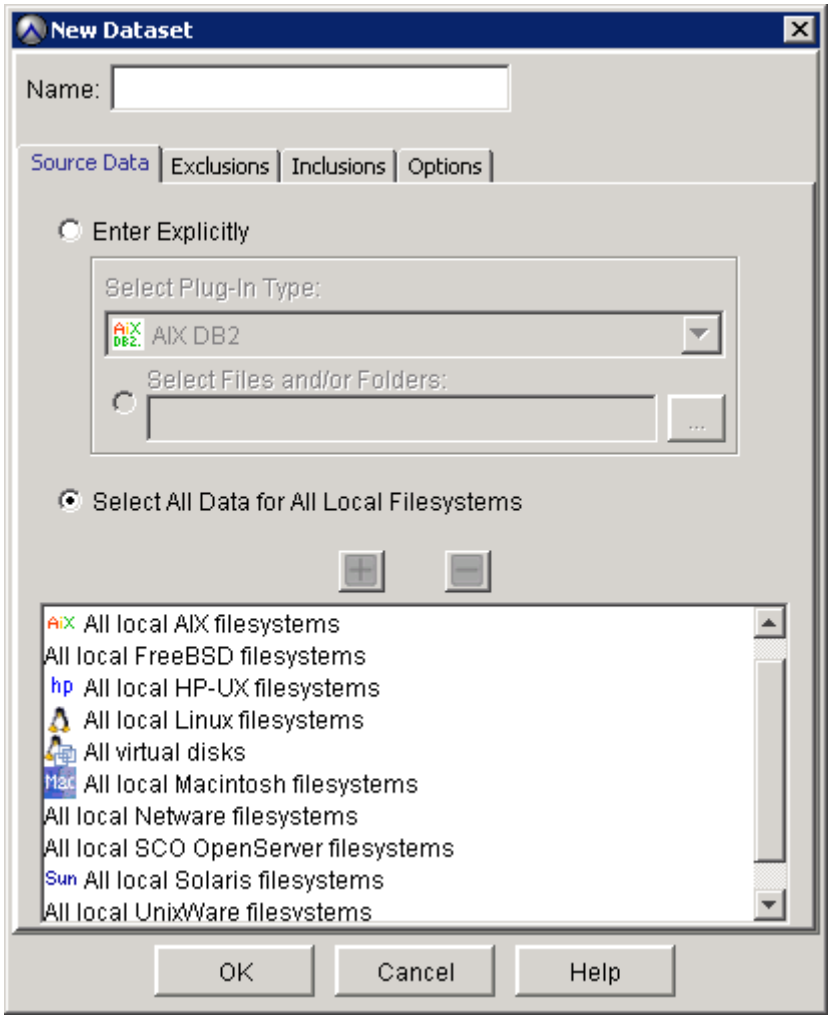


Figura 5. Creación de nuevo conjunto de datos.

6.2.5.6.2 Calendario

Un calendario es un objeto que define la planificación del respaldo de un cliente. En Avamar el concepto de calendario es distinto al concepto tradicional de calendario de otras soluciones de respaldo.

Hay que tener en cuenta los siguientes conceptos:

- Hora de inicio: define la hora inicial más temprana a la que se puede iniciar esa actividad.
- Hora de fin: define la hora de fin más tardía en la que esa actividad puede terminar.
- Duración: número de horas que puede durar esta actividad (trabajo) antes de que el sistema la finalice, independientemente de si ha terminado o no.
- Recurrencia: número de días por día o semana que se iniciará esta actividad

En el Servicio, la ventana de respaldo debe entenderse como el tiempo comprendido entre la hora de inicio y la duración. En la práctica, las actividades programadas rara vez comienzan o terminan a tiempo. La hora de inicio se ve afectada por la carga del servidor y la hora de fin se ve afectada por la complejidad de la tarea (cantidad de datos nuevos de cliente, número de grupos a ejecutar, etc.).

Existen tres opciones iniciales para definir la recurrencia en un calendario:

- Repetir diariamente: permite elegir recurrencia en base a varias horas del día.
- Repetir semanalmente: permite elegir recurrencia en base a varios días de la semana.
- Repetir mensualmente: permite elegir recurrencia en base a criterios mensuales (primer lunes del mes por ejemplo).
- Repetir bajo demanda: en este caso, el calendario no se ejecutará, pero queda definido.

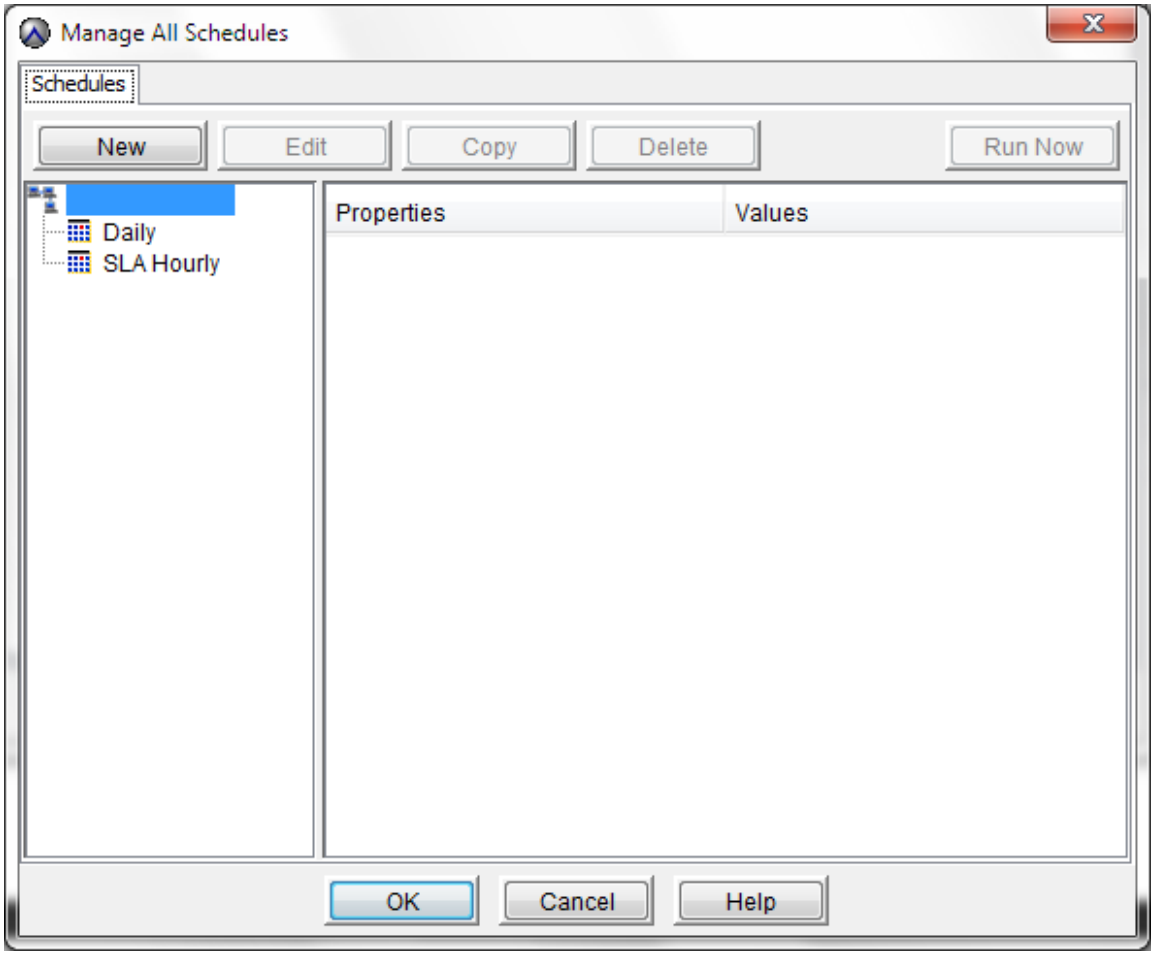
Las restricciones de activación (*Activation constrains*) definen cuando se activará ese calendario:

- *Delay until* (fecha): permite dejar el calendario inactivo hasta la fecha indicada.
- *No end date*: se activa sin fecha de fin.
- *End after* (fecha): se activa hasta la fecha indicada.

Avamar provee cinco calendarios por defecto que se pueden utilizar como base para configurar nuevos calendarios.

El cliente podrá crear calendarios dentro de su dominio.

La recomendación es crear el menor número de calendarios posible ya que se complica la gestión para el cliente.



6.2.5.6.3 Políticas de retención

Las políticas de retención permiten especificar durante cuánto tiempo se almacena una copia de respaldo en el sistema. Una vez expira una copia de respaldo, el sistema lo marca como para borrado, y se borrará durante las ventanas de mantenimiento.

El propósito principal de una política de retención es definir una fecha de expiración para una copia de respaldo.

Los parámetros básicos que definen una política de retención son:

- Periodo de retención (*Retention Period*): define un periodo fijo de retención en base a la fecha de inicio de una copia de respaldo en particular. Puede expresarse como cualquier combinación de días, semanas, meses o años.
- Fecha de fin (*End date*): permite asignar una fecha concreta como fecha de expiración.
- Sin fecha de fin (*No end date*): esta opción permite guardar las copias de respaldo de manera indefinida.

Los parámetros avanzados permiten definir con una granularidad mayor la fecha de expiración basándose en el número de copias de respaldo diarias, semanales, mensuales y anuales que se quieran retener en el sistema. Este parámetro enlaza con la configuración de periodicidad definido en los calendarios. Las opciones avanzadas de

retención están recomendadas para respaldos diarios en conjunción con el uso de calendarios y nunca son aplicables a respaldos bajo demanda.

Avamar provee cinco tipos de retención por defecto que se pueden utilizar como base.

El cliente podrá crear políticas de retención dentro de su dominio.

La recomendación es crear el menor número de políticas de retención posible ya que se complica la gestión para el cliente.

6.2.5.6.4 Ventanas de operación

Existen tres ventanas de operación en el sistema:

- Ventana de respaldo**:** el sistema no hace tareas de mantenimiento. Se pueden hacer copias de respaldo y restauraciones hasta el límite de hilos del sistema.

- Ventana de apagón (*Blackout*): durante la ventana de apagón se ejecutan tareas de *garbage collection* (borrado de copias de respaldo expirados) y se crea un punto de control o *checkpoint* que permite restaurar el sistema a ese punto en el tiempo. Durante esta ventana, el sistema entra en modo de solo lectura, con lo cual no se pueden realizar respaldos, aunque sí restauraciones. La duración de la ventana de apagón es de tres horas.

- Ventana de chequeo (*healthcheck*): durante esta ventana el sistema crea y válida un punto de control. La duración de la ventana de chequeo será inicialmente de cinco horas. Durante este periodo el número de hilos para copias de respaldo y restauraciones se reduce considerablemente.

La tabla muestra el número de hilos de respaldo y restauración por nodo. Para el servicio, como se dispone de tres nodos de almacenamiento, las cifras se multiplican por tres (hasta un máximo de 250 hilos por sistema en caso de ampliación).

Un hilo se traduce en un trabajo de respaldo. Si no hay hilos disponibles en algún momento, esos trabajos se encolan.

	Ventana de respaldo	**Ventana de apagón**	**Ventana de chequeo**
Hilos de respaldo por nodo	17	0	2
Hilos de restauración por nodo	1	18	1

Tabla 2. Relación de hilos de ejecución por ventana de operación.

Las ventanas de operación se configurarán de la siguiente manera:

	Inicio	Fin
Ventana de respaldo	16:00	08:00
Ventana de apagón	08:00	11:00
Ventana de chequeo	11:00	16:00

Tabla 3. Horario de las ventanas de operación.

Es necesario destacar, que durante la ventana de respaldo, con la configuración inicial con la que arrancará el servicio de tres nodos de almacenamiento, el número de trabajos de respaldos simultáneos es de 51 y el número de trabajos de restauración es de 3. A partir de esas cifras, los trabajos se encolarán.

Durante la ventana de chequeo y con la configuración inicial de tres nodos de almacenamiento, el número de trabajos de respaldo simultáneos es de seis y el número de trabajos de restauración es de tres. A partir de esas cifras, los trabajos se encolarán.

Si se programa un respaldo o se lanza una copia de respaldo bajo demanda durante la ventana de apagón, el sistema cancelará ese trabajo y aparecerá como fallido en la consola de Avamar.

Si se está ejecutando un respaldo y comienza la ventana de apagón el trabajo quedará en pausa hasta que el sistema salga del modo solo lectura.

6.2.6 Componentes lógicos Data Protection Advisor

6.2.6.1 Servidor virtual dbdpa

Máquina virtual alojada en el servicio de hosting virtual.

Sobre esta máquina se ejecuta una instancia del Gestor de Bases de Datos Relacional Microsoft SQL Server que contiene las bases de datos con las que trabaja Data Protection Advisor. También se ejecutan los servicios de Data Protection Advisor.

6.2.6.2 Instancia de SQL Server

Como se ha comentado anteriormente, la base de datos donde se van a almacenar los datos recopilados por DPA para su posterior análisis han de almacenarse en una base de datos externa.

Al tratarse de un entorno Windows, a continuación se detalla cómo configurar una base de datos Microsoft SQL para poder utilizarla como repositorio de DPA. El servidor SQL puede instalarse en la misma máquina que el servidor de DPA o en una distinta. DPA puede autenticarse contra el servidor de SQL utilizando autenticación Windows o autenticación propia de SQL.

El primer paso sería instalar el software de SQL Server, aceptando las opciones por defecto. A continuación se configurará el modo de autenticación, para ello se seguirán los siguientes pasos:

1. Seleccionar ***Programas > Microsoft SQL Server > SQL Server Management Studio*** dentro del menú de Inicio.
2. Dentro del SQL Server Management Studio, se seleccionará el servidor de base de datos (el primer elemento dentro de la estructura).
3. Se hará clic con el botón derecho y se selecciona ***Properties***. La ventana que aparecerá muestra las propiedades del servidor, como se muestra en la siguiente figura.
4. A continuación se seleccionará la ventana de Security.
5. Es en esta página donde se seleccionará el método de autenticación deseado. Se seleccionará *SQL Server and Windows Authentication mode* para un modo mixto de autenticación, *o Windows authentication mode* para un modo de autenticación propio de Windows.
6. Se hará clic en Ok.

Una vez configurado el modo de autenticación, se pasará a la creación de las bases de datos. Se ha de tener en cuenta que si se está utilizando un método de autenticación propio de SQL, las bases de datos, así como los usuarios necesarios han de crearse manualmente antes de la instalación del servidor de DPA. Por el contrario, si el método de autenticación elegido es Windows, las bases de datos se crearán durante la instalación de DPA. A continuación se enumeran los pasos necesarios para la creación de las bases de datos:

1. Seleccionar ***Programas > Microsoft SQL Server > SQL Server Management Studio*** dentro del menú de Inicio.
2. Seleccionar *New Database* dentro del menú en la estructura de bases de datos. Se mostrará la ventana de propiedades de la base de datos.
3. Introducir el nombre de la base de datos de configuración (*config* es el nombre por defecto).

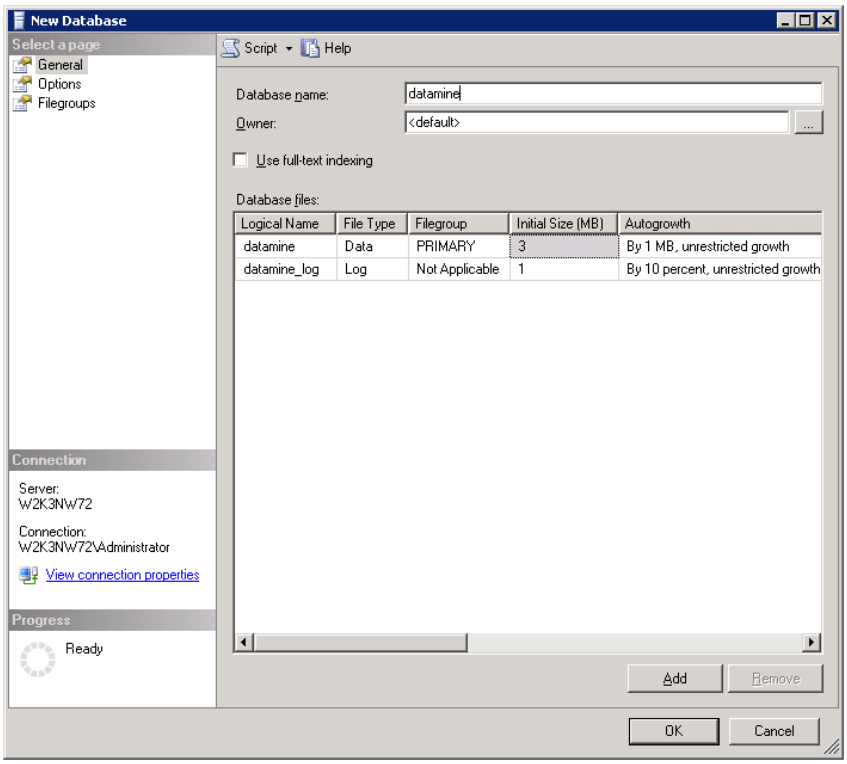


Figura 6. Creación de nueva Base de Datos.

4. Se hará clic en Ok.
5. Se repetirán estos mismos pasos para la creación de la base de datos *datamine.*

Por último, habrá que crear los usuarios necesarios para acceder a las bases de datos creadas anteriormente. Para ello, se seguirán los siguientes pasos:

1. Seleccionar *Logins* dentro de la estructura de *Security*.
2. Hacer clic con el botón derecho y seleccionar *New Login*. Se introduce el nombre del usuario que gestionará la base de datos de configuración (el nombre por defecto es *config*), como se muestra en la siguiente figura:

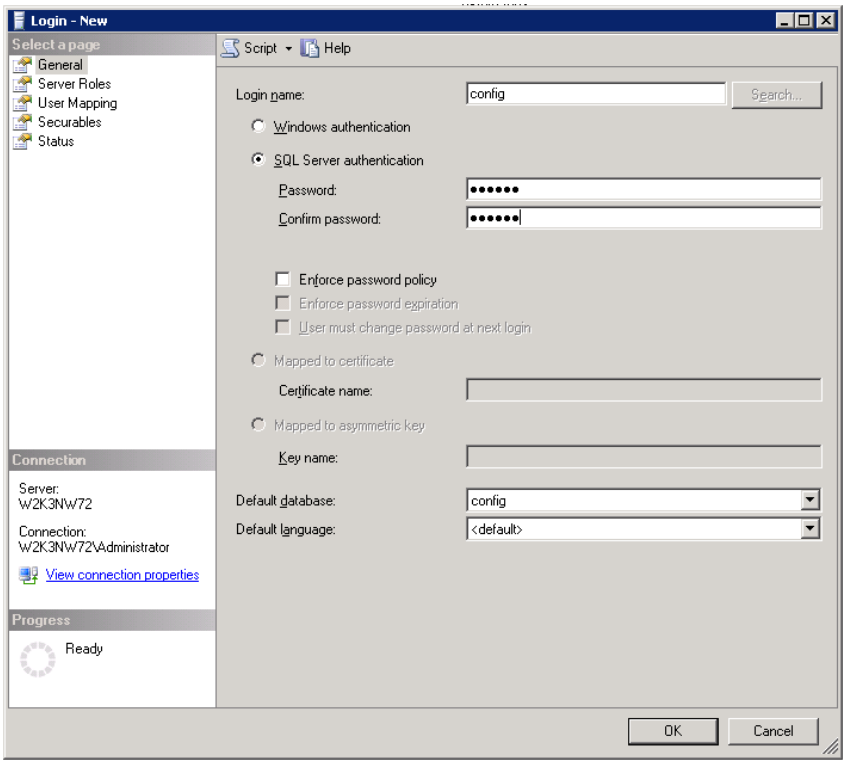


Figura 7. Creación de nuevos usuarios.

1. Se selecciona *SQL Server authentication*.
2. Se introducirá la contraseña en los campos de *Password* y *Confirm Password*.
3. Deberá limpiar la casilla de verificación de *Enforce password policy*, ya que por defecto viene seleccionado.
4. Se selecciona la base de datos de configuración creada en los pasos anteriores.
5. Se selecciona la ventana de *User Mapping* y se especifican los permisos para el usuario.
6. Se activará la casilla de verificación de la base de datos de configuración
7. Se activará la casilla de verificación de permisos del usuario *db_owner*.
8. Se hará clic en Ok.
9. Habrá que repetir los pasos 1-8 para crear y dar permisos al usuario que gestione la base de datos *datamine*.

6.2.6.3 Vistas y menús

Se creará una vista para cada cliente que sólo muestre el dominio, clientes y grupos de ese cliente.

Se creará un menú que muestre únicamente los informes visibles para el cliente.

6.2.6.4 Usuarios y roles

Cada cliente del servicio tendrá un usuario para conectarse a la consola de DPA que se creará en tiempo de provisión del cliente. Este usuario estará asociado a su rol de cliente con acceso restringido únicamente a su propia vista, menús e informes.

6.2.6.5 Informes

El cliente podrá acceder a la consola de Data Protection Advisor para consultar sus informes a través de la URL http://dbdpa.proveedordeservicio.org:9002

Figura 8. Pantalla de bienvenida a Data Protection Advisor

Necesitará un usuario y contraseña de acceso para iniciar la aplicación Java que da acceso a los informes.

Figura 9. Ventana de autenticación de Data Protection Advisor

Además, el cliente también podrá planificar sus informes para que se generen automáticamente y se le envíen por correo electrónico.

A continuación se listan los informes a los que tendrá acceso el cliente.

6.2.6.5.1 Informe de todos los Trabajos (*All Jobs*)

Distribución: cliente
Ejemplo:

Server	Domain Name	Media Server	Group	Schedule	Client	Job	Status	Error Code	Error Code Summary	Status Code	Status Code Summary	Level	Size (GB)	Files	Num Files Not Backed Up	Started	Finished	Duration (day)	Throughput (MB/sec)	Retention (week)
ava-jc8-1-uti.telefonica.es	ITSOL	ava-jc8-1-uti.telefonica.es	Admin On-Demand Group	Admin On-Demand Schedule	tzpc102655.tsol.corp	Windows File System-/Client On-Demand Data	success	0	Administrative code.	30000	Activity completed successfully.	Full	0,0	1	0	21/06/11 17:50 CEST	21/06/11 17:51 CEST	38 seconds	0,0	8 weeks 3 days
ava-jc8-1-uti.telefonica.es	ITSOL	ava-jc8-1-uti.telefonica.es	Admin On-Demand Group	Admin On-Demand Schedule	tzpc102655.tsol.corp	Windows File System-/Client On-Demand Data	success	0	Administrative code.	30000	Activity completed successfully.	Full	0,0	1	0	21/06/11 17:53 CEST	21/06/11 17:53 CEST	13 seconds	0,1	8 weeks 3 days
ava-jc8-1-uti.telefonica.es	ITSOL	ava-jc8-1-uti.telefonica.es	Admin On-Demand Group	Admin On-Demand Schedule	tzpc102655.tsol.corp	Windows File System-/Client On-Demand Data	success	0	Administrative code.	30000	Activity completed successfully.	Full	0,0	1	0	21/06/11 17:54 CEST	21/06/11 17:54 CEST	10 seconds	0,0	8 weeks 3 days
ava-jc8-1-uti.telefonica.es	ITSOL	ava-jc8-1-uti.telefonica.es	EXCHANGE	Alas 04_00	ex2k10bz01.ex2k10.local	Windows Exchange 2007-2010 VSS-ALL	failed	10001	Command failed: Miscellaneous error.	30999	Activity failed - client error(s).	Full	0,0	0	0	21/06/11 04:00 CEST	21/06/11 04:00 CEST	5 seconds	0,0	
ava-jc8-1-uti.telefonica.es	ITSOL	ava-jc8-1-uti.telefonica.es	EXCHANGE	Alas 04_00	ex2k10bz01.ex2k10.local	Windows Exchange 2007-2010 VSS-ALL	success	0	Administrative code.	30000	Activity completed successfully.	Full	0,0	222	0	22/06/11 04:00 CEST	22/06/11 04:02 CEST	1 minute 35 seconds	0,0	8 weeks 3 days
ava-jc8-1-uti.telefonica.es	ITSOL	ava-jc8-1-uti.telefonica.es	EXCHANGE	Alas 04_00	ex2k10bz01.ex2k10.local	Windows Exchange 2007-2010 VSS-ALL	success	0	Administrative code.	30000	Activity completed successfully.	Full	0,0	212	0	23/06/11 04:00 CEST	23/06/11 04:01 CEST	1 minute 33 seconds	0,0	8 weeks 3 days
ava-jc8-1-uti.telefonica.es	ITSOL	ava-jc8-1-uti.telefonica.es	EXCHANGE	Alas 04_00	ex2k10bz01.ex2k10.local	Windows Exchange 2007-2010 VSS-ALL	success	0	Administrative code.	30000	Activity completed successfully.	Full	0,0	210	0	24/06/11 04:00 CEST	24/06/11 04:02 CEST	1 minute 37 seconds	0,0	8 weeks 3 days
ava-jc8-1-uti.telefonica.es	ITSOL	ava-jc8-1-uti.telefonica.es	EXCHANGE	Alas 04_00	ex2k10bz01.ex2k10.local	Windows Exchange 2007-2010 VSS-ALL	success	0	Administrative code.	30000	Activity completed successfully.	Full	0,0	210	0	25/06/11 04:00 CEST	25/06/11 04:02 CEST	1 minute 48 seconds	0,0	8 weeks 3 days

Información que ofrece: muestra de un vistazo como han ido los trabajos del último día, incluyendo duración del trabajo, finalización, código de error e información salvada

6.2.6.5.2 Informe de Respaldos en formato Tarjeta (*Backup Report Card*)

Distribución: cliente
Ejemplo:

Node	20 jun	21 jun	22 jun	23 jun	24 jun	25 jun	26 jun
Nodo1							
Nodo2							
Nodo3							
Nodo4							
Nodo5							

Color	Description
	Successful backup
	Failed backup
	Missed backup
	No backup information

Información que ofrece: muestra en una tabla un resumen de ejecución de todos los trabajos de respaldo de la última semana. En color verde tendríamos los trabajos de copia de respaldo finalizados con éxito, y en rojo los terminados con algún tipo de fallo. Si en la misma celda aparecen tanto rojo como verde, significa que esa máquina tiene instalado más de un agente de Avamar y que algún trabajo ha fallado o se ha ejecutado más de un respaldo ese día y alguno ha fallado.

6.2.6.5.3 Informe Resumen (*Backup Client Summary*)

Distribución: cliente
Ejemplo:

Completed	Successful	Partial	Failed	Missed	Active	Success Rate (%)
5	1	3	1	0	0	20,00

Información que ofrece: muestra de un vistazo el número de trabajos de copia de respaldo terminados con éxito, fallados, activos, etc.

6.2.6.5.4 Informe de Tasa de Cambios por Cliente (*Backup Job Change Ratios by Client*)

Distribución: cliente
Ejemplo:

Server	Client	Protected (GB)	Last Incremental Size (GB)	Last Incremental Rate (%)	Average Incremental Size (GB)	Average Incremental Rate (%)	Total Size (GB)	Size Rate (%)
Avaserver1	Nodo1	0,0z	0,0	0,0	0,0	33,3	0,0	100,0
Avaserver1	Nodo2	582,3	33,4	5,7	14,2	2,4	99,6	17,1

Información que ofrece: muestra el espacio protegido por cada cliente del que se hace respaldo.

6.2.6.5.5 Informe Tasa de Cambios agregada (*Aggregate Backup Job Change Ratios*)

Distribución: cliente
Ejemplo:

Protected (GB)	Last Incremental Size (GB)	Last Incremental Rate (%)	Average Incremental Size (GB)	Average Incremental Rate (%)	Total Size (GB)	Size Rate (%)
582,3	33,4	5,7	14,2	2,4	99,6	17,1

Información que ofrece: muestra el sumatorio de espacio protegido de todos los clientes de respaldo de un cliente del servicio.

6.2.6.6 Alertas de exceso de espacio contratado

Por cada cliente, se configurará un monitor en DPA que compruebe cada cuatro horas si el espacio protegido total en su dominio supera el espacio contratado.

La base para el monitor es el informe del apartado 6.2.6.5.5, el cual muestra el total de espacio protegido por todos los clientes de respaldo de un cliente del servicio.

Si la condición se cumple, es decir, el cliente protege más espacio del que tiene contratado, DPA enviará un correo electrónico a la dirección del grupo de administración del Servicio de Respaldo en la Nube del Proveedor de Servicio, grupo que será responsable de informar al responsable del servicio para que comunique la situación irregular al cliente.

6.2.7 Monitorización

Para monitorizar la plataforma del Servicio se configurarán las siguientes alertas que recibirá el grupo técnico encargado de su administración y mantenimiento en su dirección de correo electrónico.

Las alertas configuradas son:

Código de Error	Mensaje de Error
1	Internal server error
4004	hfscheck_cron: failed hfscheck of $chkpt
4202	failed garbage collect
4302	cp_cron: failed checkpoint maintenance
4303	cp_cron: MC checkpoint task failed
4304	cp_cron: EM checkpoint task failed
5073	restore failed (frompath:%d)
10011	Command failed: Restore failed
10016	Command failed: Session cancelled by Server
10019	Command failed: Externally cancelled by Administrator
22310	Change of the scheduler status to suspended or resumed failed
22407	Flush of Administrator Server data to server is overdue
22408	A checkpoint of server data is overdue
22409	A checkpoint validation (hfscheck) of server checkpoint data is overdue
22415	The server is approaching full capacity
22416	The server storage has exceeded maximum operating capacity
22605	A server node has gone offline
22609	A error occurred creating a server checkpoint
22614	Errors were found validating a server checkpoint
22629	Server is approaching capacity (use parameter tab to set % value)
22630	Server has reached capacity
22713	Syslog error message: %s
22905	Event email notification failed

Respecto a la monitorización del servidor de DPA, cada grupo técnico se encargará de la monitorización de sus elementos, el grupo de Sistemas Windows monitorizará el porcentaje de ocupación de los discos, los servicios críticos de sistema y los porcentajes de utilización de CPU y memoria, y el grupo de bases de datos monitorizará el estado de las bases de datos de SQL Server.

El grupo de administración del Servicio de Respaldo en la Nube recibirá notificaciones por correo sobre el estado de los servicios relativos a DPA.

6.2.8 Baja del servicio

La baja del servicio se realizará de forma progresiva ya que el cliente debe ser capaz de hacer restauraciones de las copias de respaldo que se hayan hecho hasta la fecha de la baja. El cliente accederá con permisos de sólo restauración ("*restore only*") mientras expira el último respaldo realizado antes de la baja.

Los pasos para la baja serán los siguientes:

1. Se notifica al grupo de administración del Servicio de Respaldo en la Nube la baja del cliente.
2. El grupo de administración cambia el rol del usuario *admin* del dominio del cliente a "*restore only operator*".
3. Desde la ventana de Políticas de Avamar, el grupo de administración del Servicio de Respaldo en la Nube editará los grupos y clientes del dominio del cliente marcando la opción "*disabled*" para cancelar los futuros trabajos de respaldo.
4. El grupo de administración del Servicio de Respaldo en la Nube comprobará a través de DPA, qué respaldo expira más tarde. Hasta que llegue esa fecha el cliente será capaz de realizar restauraciones de los respaldos realizados hasta el día de la baja.

Una vez llegue la fecha de expiración, el grupo de administración del Servicio de Respaldo realizará las siguientes tareas:

1. Eliminar todos los usuarios de dominio.
2. Pasados tres meses de la expiración del último respaldo se eliminarán los clientes y el dominio de cliente.

6.3 Manual técnico de Operación

El servicio es contratable por cualquier cliente que sea capaz de alcanzar las máquinas del Servicio cuyas direcciones IP están publicadas en Internet. De igual forma, podrán acceder al servicio clientes que accedan a los CPDs del Proveedor de Servicios a través de una extensión de LAN o cualquier otro tipo de conexión que permita extender redes.

El servicio está basado en un modelo de administración delegada al cliente (*Software as a Service*), lo que supone lo siguiente:

- El cliente es responsable de la gestión de su dominio de cliente.
- La instalación y actualización de agentes software deberá ser efectuada por el cliente.
- En el supuesto de una actualización de la infraestructura del servicio que obligue a una subida de versión de los agentes de respaldo, la actualización de los mismos será responsabilidad del cliente.
- El Proveedor de Servicios dará soporte reactivo a la instalación de agentes previa solicitud vía herramientas oficiales del Proveedor de Servicios.
- El Proveedor de Servicios no contempla asistencia "*onsite*" en las instalaciones del cliente.
- Dado que el cliente gestiona los servidores y los agentes instalados, el Proveedor de Servicios únicamente proporcionará reporte del estado de copias de respaldo satisfactorias. No se iniciará un proceso de estudio/resolución ante un fallo de salvado a menos que se trate de un fallo provocado por la infraestructura del servicio.
- Dado que el cliente gestiona los servidores origen y los agentes software instalados, el Proveedor de Servicios únicamente proporcionará reporte del estado de los respaldos efectuados, pero no tratará los respaldos fallidos de un modo proactivo, sino que deberá ser el cliente el que, vía herramientas oficiales, informe de cualquier incidencia en las copias de respaldo.
- El servicio no es responsable de la validez o consistencia de la información salvada. El cliente es responsable de validar mediante pruebas de recuperación periódicas que la información salvada es válida y consistente.
- El Proveedor de Servicios tratará incidencias en 8x5 a través de las herramientas oficiales.
- El Proveedor de Servicios no dará soporte a restauraciones.
- Los respaldos y restauraciones iniciados desde la consola cliente de Avamar no están soportados y por tanto, no se asegura ni la consistencia ni la finalización correcta de los mismos.
- El servicio no será responsable de proporcionar infraestructura adicional de comunicaciones de ningún cliente. La infraestructura del servicio es accesible desde Internet, con lo cual, el cliente es responsable de resolver la comunicación extremo a extremo entre sus máquinas y las máquinas de la infraestructura del servicio.

6.3.1 Procedimiento de Atención de Incidencias

Los procedimientos de Atención Postventa y Gestión de Incidencias serán los mismos existentes actualmente para cualquier otro servicio del Proveedor.

Los flujos posibles de atención a incidencias son tres:

- **Incidencia detectada por los sistemas de monitorización del servicio**. En este caso, la incidencia es detectada internamente, se registra en la herramienta de incidencias, y se inicia su resolución aunque el cliente no haya notificado la misma. En este caso, el grupo de Operación recibe la alarma, identifica que se trata del servicio de Respaldo en la Nube, y se traslada al grupo de administradores. Una vez resuelta, es devuelta al Operación que verifica la desaparición de la alarma y resuelve la incidencia.
- **Incidencia comunicada por el cliente a través del Centro de Relación de Clientes**. El Centro de Relación de Clientes identifica que el servicio al que se refiere el cliente es un servicio de Respaldo en la Nube, y se traspasa al Operación, que a su vez lo transfiere al grupo de administradores del servicio. Una vez resuelta la incidencia, esta es devuelva al Centro de Relación de Clientes que verifica con el cliente el cierre de ésta. Este es el procedimiento estándar de registro de incidencias de clientes.
- **Algunos clientes disponen de acceso directo a la herramienta de incidencias**. Estos clientes pueden introducir directamente la incidencia en este sistema. Esta incidencia le llega a Operación, que verifica que se trata de un servicio de Respaldo en la Nube y lo propaga al grupo de administradores del Servicio. Una vez finalizada la incidencia, es devuelta al Operación que procede a su cierre.

6.3.1.1 Notificación administradores

Operación notificará las alarmas que reciban vía correo electrónico durante el horario laboral normal a los administradores de la plataforma cuyos contactos son:

Número de Teléfono: 91 XXX XX XX
E-mail: respaldoenlanube@proveedordeservicios.org

Se indicará telefónicamente la alerta motivo de la llamada y se enviará vía e-mail la transcripción de la misma.

6.3.1.2 Guardias

El grupo de Operación del Proveedor de Servicios notificará las alarmas que reciban vía correo electrónico fuera del horario laboral normal a la guardia de la plataforma cuyos contactos son:

Número de Teléfono: 91 XXX XX XX
E-mail: respaldoenlanube@proveedordeservicios.org

Indicándoles telefónicamente la alerta motivo de la llamada y enviándoles vía e-mail la transcripción de la misma.

6.3.2 Operativas

6.3.2.1 Descarga de la consola de Avamar

Para tener acceso a la consola de administración de Avamar, es necesario descargar e instalar el software desde la web que publica el Servicio para distribuir documentación y software.

Para ello, hay que apuntar un navegador a la dirección http://backupenlanube.proveedordeservicios.org y seleccionar el enlace *Documents and Downloads* que conducirá página de descargas:

Name	Last Modified	Size
AvamarBackupSystemState-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	54.1M
AvamarClient-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	15.5M
AvamarClientCluster-windows-x86-4.1.101-340.exe	20-Mar-2009 16:10	9.2M
AvamarConsoleMultiple-windows-x86-5.0.3-29.exe	15-Sep-2010 08:16	11.7M
AvamarExchange-windows-x86-4.1.101-340.msi	20-Mar-2009 16:10	9.5M
AvamarExchange2003-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	12.7M
AvamarLotus-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	12.6M
AvamarMoss2007-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	9.0M
AvamarRMAN-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	7.3M
AvamarSQL-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	7.5M
AvamarVmImage-windows-x86-5.0.106-28.iso	10-Sep-2010 21:20	34.7M
jre-6u12-windows-i586-p.exe	02-Mar-2009 22:36	15.5M

Figura 10. Descarga de la consola de Avamar.

Si el servidor donde se va a instalar la consola no tiene instalada la versión 6 o superior de Java, es necesario descargar e instalar el fichero jre-6u12-windows-i586-p.exe.

Para instalar la consola de Avamar en plataforma Windows x86 por ejemplo, hay que descargar e instalar el fichero "AvamarConsoleMultiple-windows-x86.exe". El asistente guía la instalación.

6.3.2.2 Conexión a la consola del Servicio

El acceso al servidor de Avamar se realiza desde la consola. Para ejecutar la consola, desde el menú inicio, navegar por *Programas, EMC Avamar, Administrator* y ejecutar *Avamar Administrator*.

Aparecerá la siguiente ventana:

Figura 11. Conexión a la consola de Avamar

Si es la primera ejecución de la consola, es conveniente configurar el servidor por defecto para no tener que rellenar esa información en cada acceso.

Para ello, pinchar en el botón "*Options*" y modificar los siguientes parámetros:

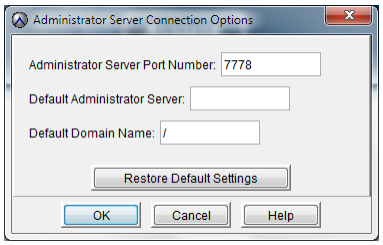


Figura 12. Parametrización de agente de Avamar

- **Default Administrator Server**: backupenlanube.proveedordeservicios.org.
- **Default Domain Name**: Introducir "/" para conectarse al nivel más alto de dominios.

El acceso al sistema se realizará con el usuario MCUser (*superadministrador*) disponible en el repositorio seguro de contraseñas.

La ventana principal de la consola de administración de Avamar consiste en un menú con las opciones de *Actions, Tools, Navigation and Help*. Así como seis botones etiquetados como *Policy, Backup & Restore, Administration, Backup Management, y Activity*.

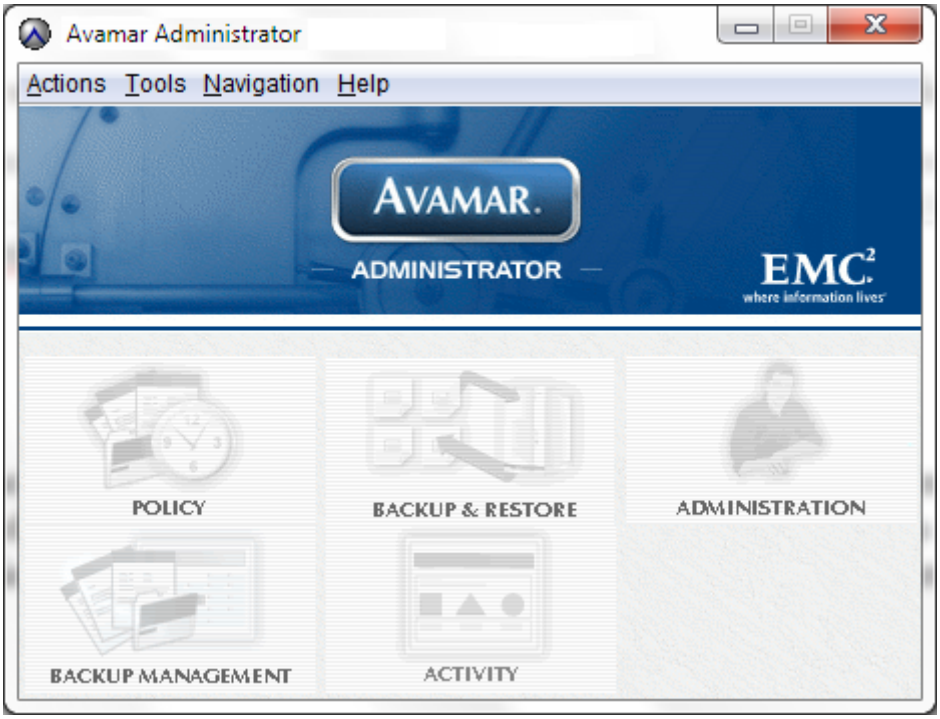


Figura 13. Consola de Administración de Avamar

En la Consola de Administración de Avamar, la estructura del dominio se muestra en muchas de las vistas disponibles, en el panel de la izquierda. Haciendo clic en el recuadro situado más a la izquierda del árbol de dominios, se expande la estructura, mostrándose los subdominios (si es que existen) y grupos y clientes que hayan sido asignados a dicho dominio.

Si ya existen usuarios adicionales al usuario *admin*, los usuarios con roles *backup only operator*, *restore only operator*, *backup/restore operator*, *activity operator* pueden iniciar sesión en la consola de administrador de la misma forma que el usuario *admin*. Las funciones estarán limitadas a las descritas en el apartado Usuarios de dominio.

6.3.3 Manual de usuario del servicio

El manual de usuario del servicio tiene operativas interesantes para el administrador del Servicio de Respaldo en la Nube, las cuales se repasan en el apartado 6.4.

6.3.4 Monitorización diaria

6.3.4.1 Avamar

La monitorización diaria de Avamar consiste en conectarse a la consola Avamar Administrator con el usuario MCUser, y desde la vista Server, pestaña Server Management comprobar:

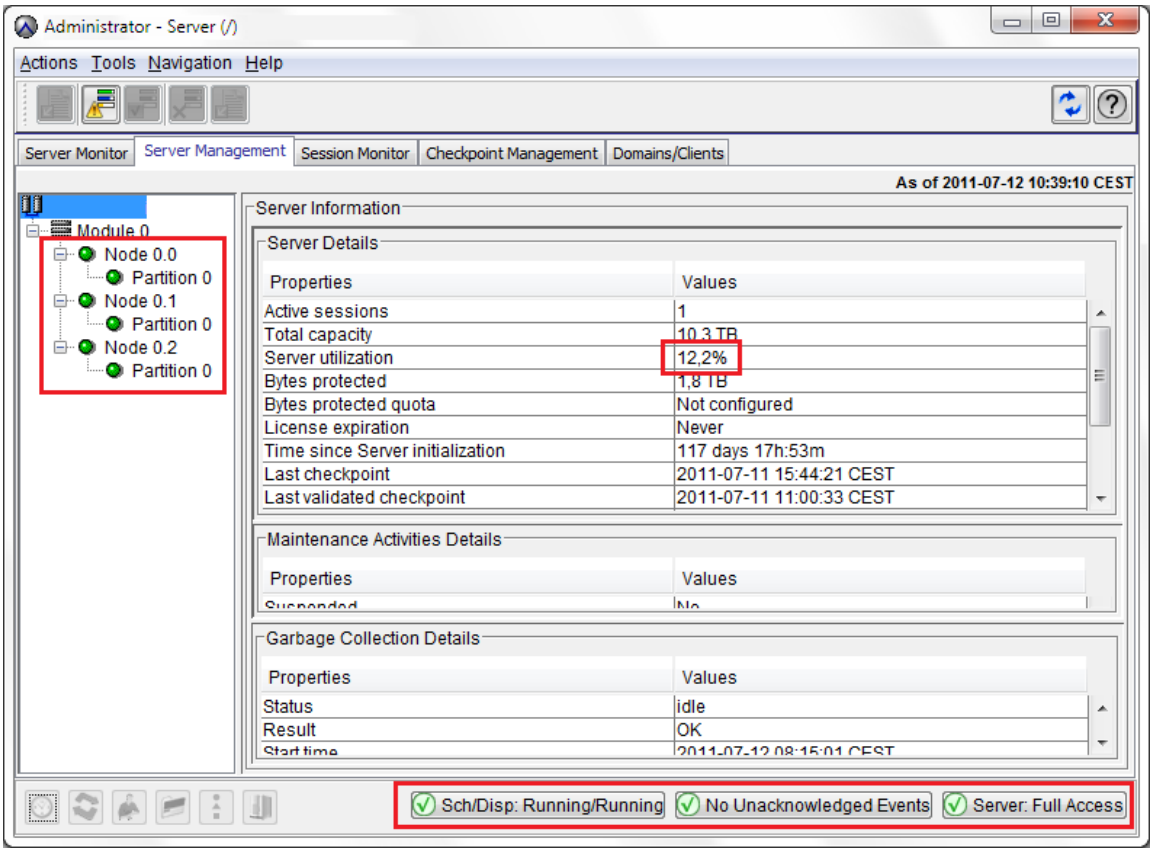


Figura 14. Comprobación de servicio de Respaldo en la Nube

1. Estado de los nodos: parte izquierda del árbol.
2. Utilización del sistema: aunque hay alarmas configuradas, si la utilización se acerca al 60% notificarlo inmediatamente al responsable del servicio.
3. Alertas generales: la parte inferior de la ventana muestra alertas generales del sistema como puede ser estado de puntos de control y otros eventos.

6.3.4.2 Data Protection Advisor

La monitorización diaria de DPA consiste en conectarse a la consola de DPA con el usuario administrador del servicio, y mostrar los siguientes informes para el periodo del último día:

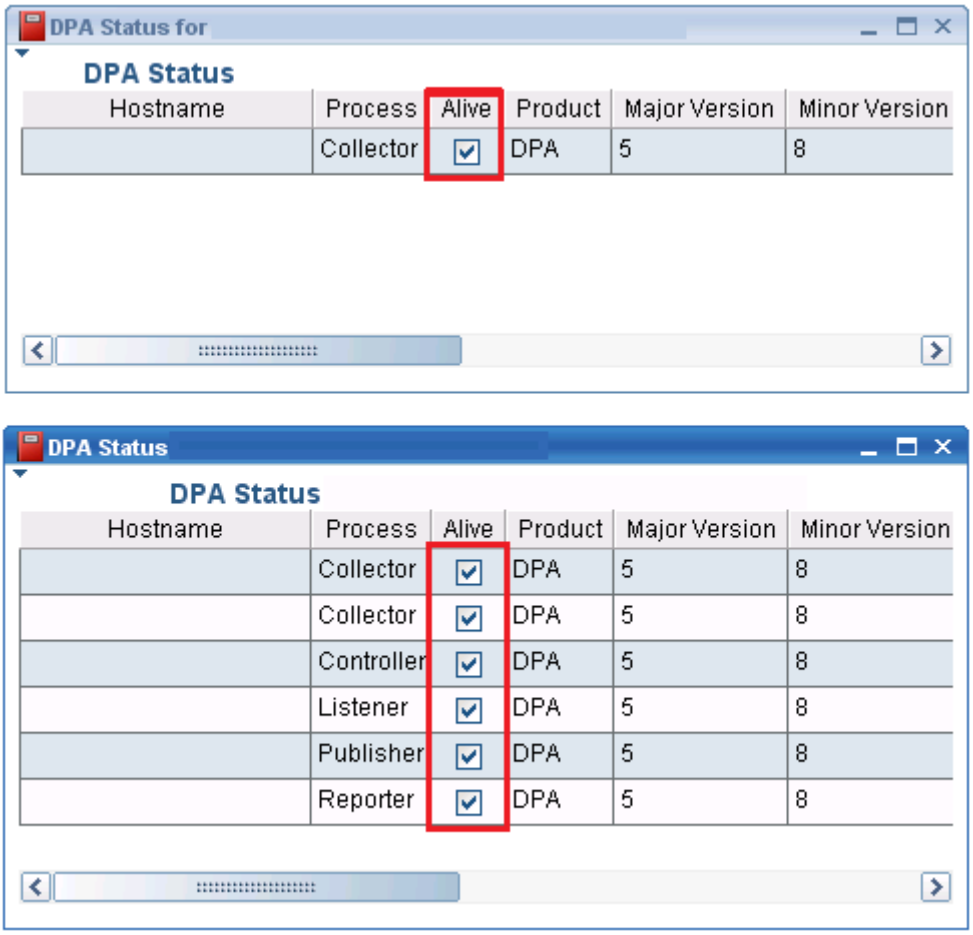


Figura 15. Comprobación de Data Protection Advisor

6.3.4.3 Respaldos en fallo del último día.

Se consultará a diario el informe de todos los trabajos para un periodo correspondiente al último día.

Si el grupo “SLA plataforma” del dominio “133794FPS” presenta algún fallo durante el último día, es necesario investigar si ha habido indisponibilidad del servicio y si hay clientes afectados y calcular las horas de cara al plan de disponibilidad mensual y cálculos de SLA.

6.3.5 Historiales (*logs*) y directorios frecuentes

- Log de sistema operativo de los nodos de Avamar: */var/log/messages.*
- Directorio de Avamar en el nodo de utilidad: */usr/local/avamar*.
- Directorio de logs de Avamar: */usr/local/avamar/var/log*.
- Colector de DPA en el nodo de utilidad:
  - Binarios: */opt/dpa.*
  - Log: */var/log/dpa/collector.log*.
  - Estado, arranque: */etc/init.d/dpa status, /etc/init.d/dpa start/stop*
- Registros de los servicios del servidor DPA: *C:\Program Files\EMC\DPA\log*
- Registros de servicio "*Backup Agent Avamar*":

1. Windows: *C:\Program Files\avs\var\avagent.log*
2. UNIX: */opt/AVMRclnt/var/avagent.log*

6.3.6 Directorio de parches de Avamar

El servicio permite al administrador actualizar parches fácilmente a través de la URL: http://backupenlanube.proveedordeservicios.org/em. Antes de instalar los parches, estos deben descargarse en un directorio del servidor donde se esté ejecutando el *DownloadService*. En este caso, el servicio se ejecuta en el servidor de DPA y el directorio de descarga es C:\DownloadService.

El grupo de administración del servicio comprobará mensualmente la ocupación de este directorio. Se considerará dentro de los límites habituales una ocupación máxima de 10GB.

6.3.7 Control de Historiales (*logs*) de seguridad

De forma semanal, los administradores del servicio de Respaldo en la Nube comprobarán la infraestructura para verificar que no ha habido ataques (Los más comunes podrían ser por métodos de fuerza bruta) contra los nodos de Avamar o DPA.

Para ello, conectarse como *root* a los nodos de Avamar y ejecutar el siguiente comando:

more /var/log/messages | grep "authentication failure"

Si se ha sufrido un ataque por fuerza bruta, el comando debería devolver una cantidad importante de líneas. Además, la marca horaria de las líneas del registro debe ser consecutiva (muchos intentos por minuto).

Respecto al servidor de DPA, conectarse por *Terminal Services*, y en el log *Security del Event Viewer* de Windows filtrar por el evento 4625. Comprobar que no hay muchos reintentos por minuto.

En caso de detectar cualquier anomalía el grupo de administración del servicio deberá tratar la incidencia como posible incidente de seguridad.

6.3.8 Cambio de contraseñas

Se modificarán las contraseñas de *root* de los nodos de Avamar y *administrator* del servidor de DPA cada 90 días como máximo.

Se utilizará la aplicación KeePass[28] para generar contraseñas válidas.

Para generar una contraseña, seleccionar *Generate Password*:

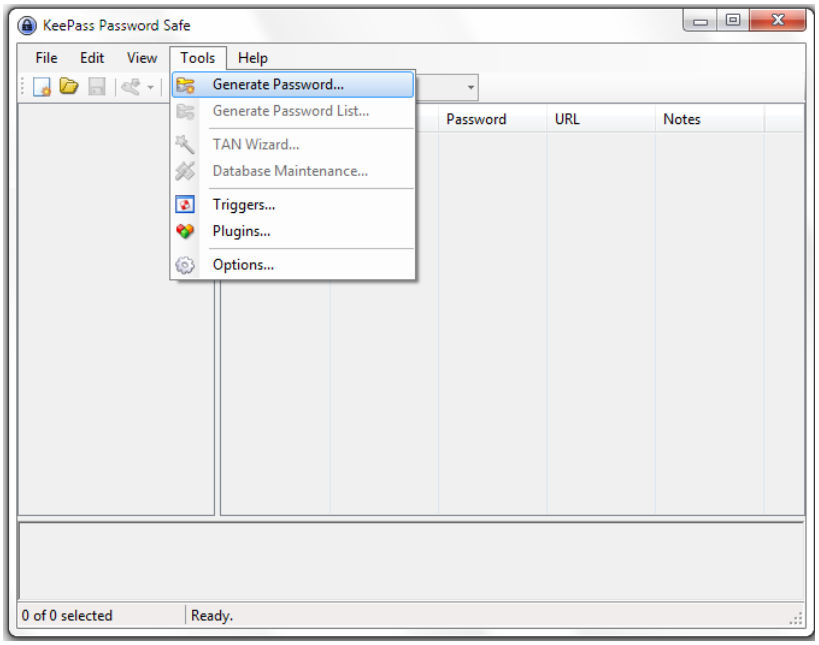


Figura 16. Generación de contraseñas en KeePass.

Seleccionar las opciones según aparecen en la siguiente captura y a continuación seleccionar la pestaña *Generate*:

Nota: no se incluirán caracteres especiales en la contraseña para evitar posibles problemas con codificaciones de caracteres.

[28] http://sourceforge.net/projects/keepass/files/latest/download?source=files

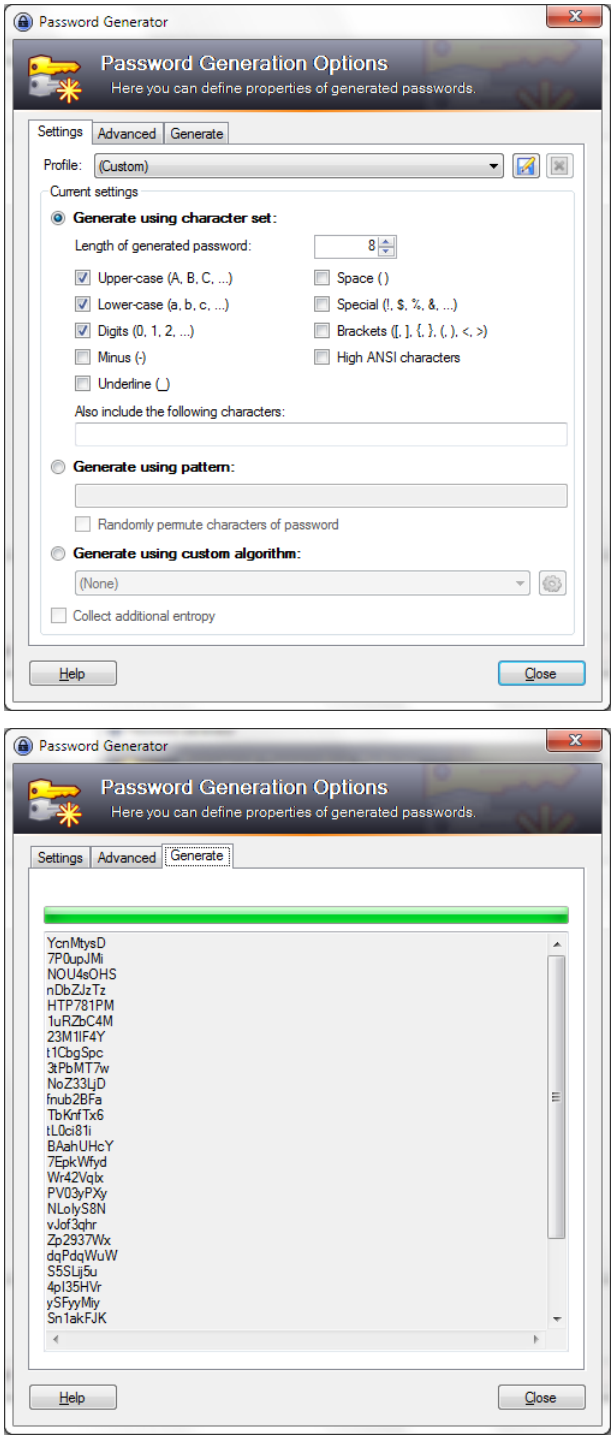


Figura 17. Selección de contraseñas seguras en KeePass.

Seleccionar una de las contraseñas generadas.

Para cambiar la contraseña del servidor de DPA, es necesario conectarse mediante Conexión a Escritorio Remoto (*Terminal Services)* de Microsoft Windows a la máquina *dbdpa* y cambiar la contraseña a través de la consola Users del servidor.

Respecto a la contraseña de los nodos de Avamar, es importante cambiar la contraseña antes de que caduque, ya que el procedimiento para cambiarla es a través del comando *change-password* de Avamar. Si la contraseña caduca, el sistema operativo de

los nodos obliga a cambiar la contraseña de *root* antes de volver a autenticarse y por tanto no permite lanzar el comando *change-password*.

El comando *change-password* permite cambiar las contraseñas de sistema operativo, de aplicación y las llaves SSH de los nodos. Únicamente es necesario cambiar las contraseñas de sistema operativo.

6.3.9 Provisión de nuevos clientes

El procedimiento completo de provisión de nuevos clientes está disponible en el apartado 6.5 del presente documento.

6.3.10 Lista de comprobaciones para el cliente

El cliente es responsable de las provisiones de sus agentes software de respaldo según lo establecido en este mismo documento en su apartado 6.3

Los siguientes apartados son una recopilación de comprobaciones rápidas para comprobar el correcto desempeño de las funciones básicas del servicio.

6.3.10.1 Resolución de nombres

El servidor donde se va a instalar la consola de Avamar o un agente de respaldo, debe resolver mediante DNS los nombres de los servidores de respaldo e informes. Para ello, desde una línea de comandos ejecutar el comando *nslookup* y preguntar por los host *backupenlanube.proveedordeservicios.org* y *dbdpa.proveedordeservicios.org*.

Si la resolución es correcta los comandos responderán respectivamente:

```
Non-authoritative answer:
Name:    backupenlanube.proveedordeservicios.org
Address:  XXX.XXX.XXX.XXX

Non-authoritative answer:
Name:    dbdpa.proveedordeservicios.org
Address:  YYY.YYY.YYY.YYY
```

Además, es necesario resolver el nombre sin añadir el dominio de host por lo que será necesario añadir las siguientes líneas en el fichero *hosts* del servidor en cuestión:

```
XXX.XXX.XXX.XXX       backupenlanube.proveedordeservicios.org backupenlanube
YYY.YYY.YYY.YYY       dbdpa.proveedordeservicios.org dbdpa
```

Nota: En servidores Windows en general, la ubicación del fichero hosts es: *%WINDIR%\System32\drivers\etc\hosts.*

En servidores UNIX (prácticamente todas las distribuciones), la ubicación del fichero es: */etc/hosts.*

6.3.10.2 Comprobación de puertos de aplicación

Para comprobar que se llega a los puertos por donde se hará respaldo y restauraciones, hay que comprobar que los siguientes comandos *telnet* se completan correctamente:

```
telnet backupenlanube.proveedordeservicios.org 27000
telnet backupenlanube.proveedordeservicios.org 28001
telnet backupenlanube.proveedordeservicios.org 29000
```

Para la consola de Avamar:

```
telnet backupenlanube.proveedordeservicios.org 7778
telnet backupenlanube.proveedordeservicios.org 7779
telnet backupenlanube.proveedordeservicios.org 7780
telnet backupenlanube.proveedordeservicios.org 7781
telnet backupenlanube.proveedordeservicios.org 80
telnet backupenlanube.proveedordeservicios.org 443
```

Para la consola de informes:

```
telnet backupenlanube.proveedordeservicios.org 9002
telnet backupenlanube.proveedordeservicios.org 3916
```

6.4 Manual técnico de Usuario

6.4.1 Acceso al portal de servicio

Para acceder a la web del servicio es necesario apuntar un navegador a la URL http://backupenlanube.proveedordeservicios.org

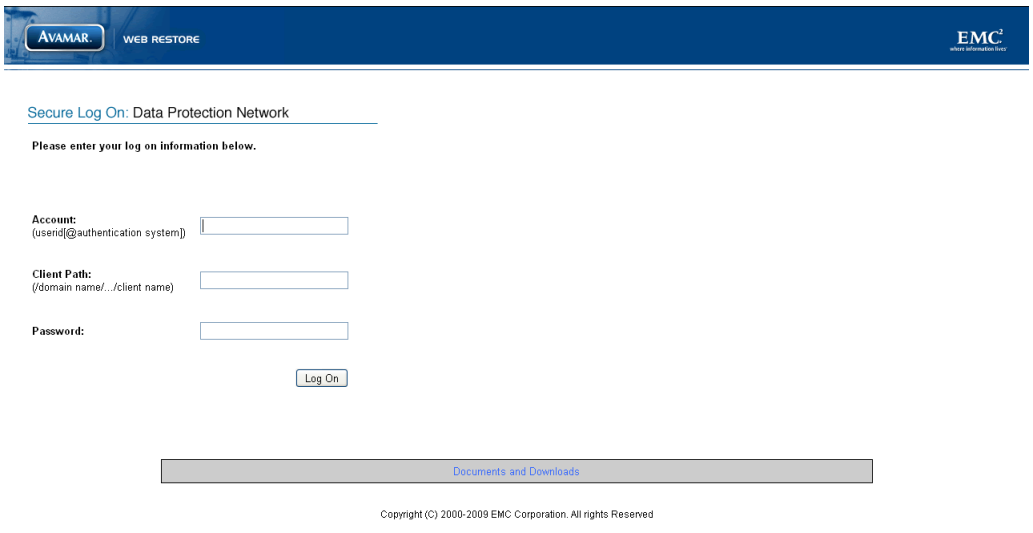


Figura 18. Portada de acceso al servicio.

6.4.2 Descarga de software y documentación de producto

Para descargar documentación adicional sobre el producto, hay que seleccionar el enlace *Documents and Downloads* que conducirá a la siguiente página:

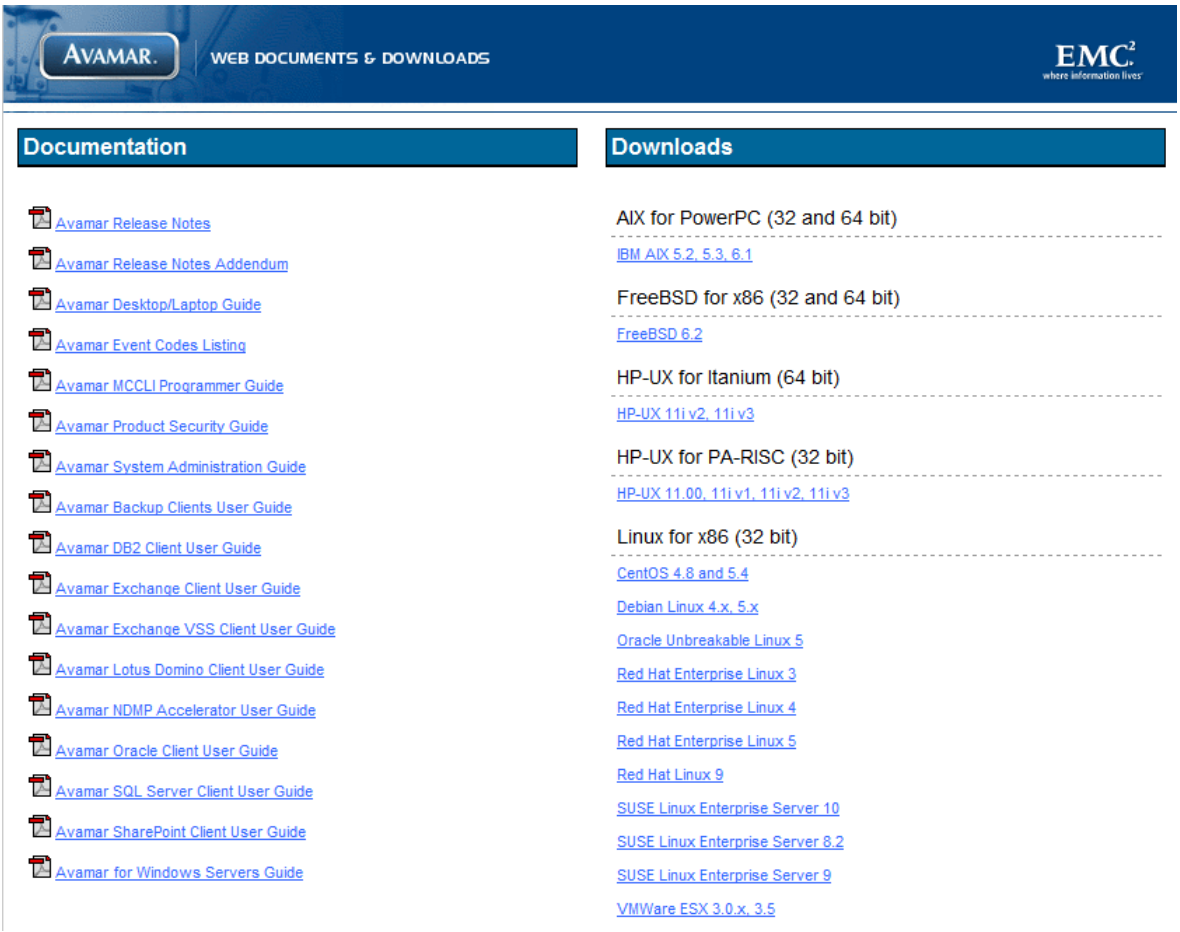


Figura 19. Descarga de agentes y documentación..

La sección de la izquierda contiene la documentación y la derecha contiene los complementos de Avamar según el sistema operativo.

La documentación adicional sobre agentes que no está disponible en esta URL, puede solicitarse vía incidencia al Proveedor.

6.4.3 Instalación de agentes

El cliente es responsable de validar la compatibilidad tanto del sistema operativo como de la aplicación de la que quiere hacer respaldo en el sistema que va a provisionar.

Previamente a la provisión de un nuevo cliente, el Gestor de Cliente recopilará información acerca del sistema en el que se va a provisionar el agente y contrastará su compatibilidad con la matriz de compatibilidad del producto.

Los entornos que se no entren dentro de la matriz de compatibilidad de Avamar no están soportados por el servicio.

6.4.3.1 Instalación del agente de Windows

Para instalar el agente hay que visitar usando un navegador web la dirección http://backupenlanube.proveedordeservicios.org y seleccionar el enlace "*Documents and Downloads*". Una vez ahí, buscar la sección de Windows y descargar el fichero *AvamarClient-windows-x86-5.0.XXX-msi*.

La instalación está guiada por el asistente:

1. Hacer clic en *Next* y aceptar el contrato de licencia:

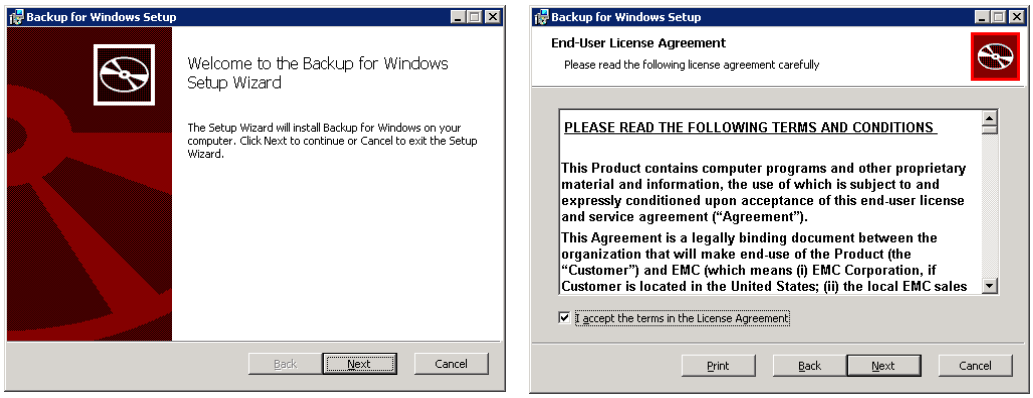


Figura 20. Instalación de agente. Aceptación de contrato.

2. Desmarcar la opción "*Desktop/Laptop Support*" ya que no está soportada por el servicio. Si se desea, se puede cambiar la ubicación de los binarios del agente. En la siguiente ventana, confirmar haciendo clic en *Install*.

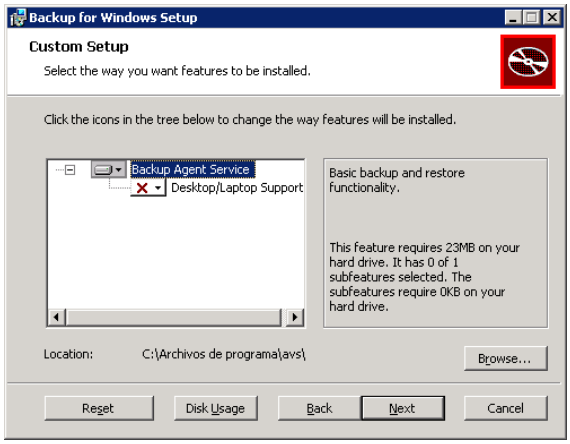


Figura 21. Instalación de agente. Funcionalidades.

3. La instalación continuará y mostrará la ventana de fin de instalación.

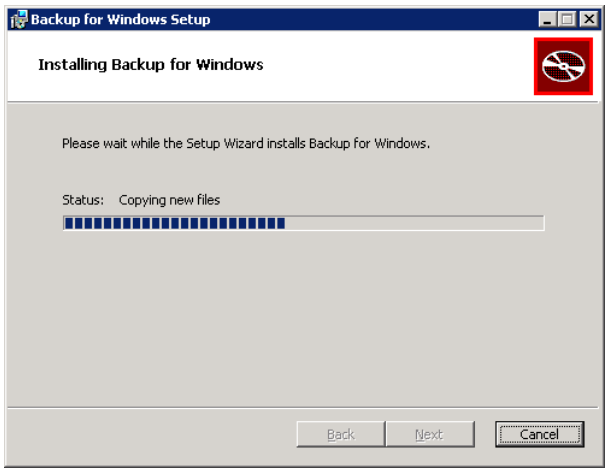


Figura 22. Instalación de agente. Fin de instalación.

4. Para comprobar que la instalación ha terminado con éxito:

    a. Ejecutar "*services.msc*" desde el menú Inicio de Windows.
    b. Comprobar que el servicio de Avamar se está ejecutando. El servicio se llama *Backup Agent*.

5. Adicionalmente, se puede comprobar mediante el Administrador de Tareas, verificando que los procesos *avagent.exe* y *avscc.exe* se están ejecutando:

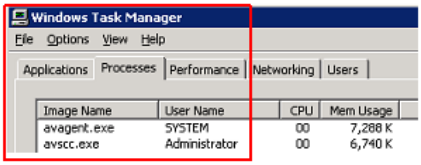


Figura 23. Instalación de agente. Comprobaciones.

6.4.3.2 Activación del cliente

El proceso de activación permite establecer una identidad con el servidor de Avamar. Una vez que el cliente está registrado, se le asigna un identificador único (*ClientID - CID*), que se envía al cliente durante la activación. Cada cliente sólo podrá estar activado en un servidor simultáneamente.

La activación del agente que se acaba de instalar se realiza desde la consola de cliente. El uso de esta interfaz sólo esta soportado en el servicio para realizar las activaciones. Los respaldos y restauraciones iniciados desde esta consola no están soportados y por tanto, no se asegura la consistencia de los mismos.

Es necesario conocer el nombre de dominio de cliente para poder activar un cliente, las activaciones en el dominio por defecto "/" no están soportadas.

Si se realiza alguna activación en el dominio por defecto, los administradores del servicio intentarán averiguar a qué cliente pertenece ese servidor. Si lo consiguen se pondrán en contacto con el administrador del cliente para informarle de que el cliente que se haya activado de forma errónea en el dominio "/" se va a mover al dominio correspondiente. Si no son capaces de averiguar el dueño de ese cliente, los administradores lo borrarán del sistema.

Para activar el agente: desde el icono de la bandeja de sistema de Windows, haciendo clic derecho, *Activate*.

En la ventana, rellenar los parámetros con la siguiente información:

- Administrator server address: backupenlanube.proveedordeservicios.org
- Client Domain: el nombre de dominio proporcionado por el Proveedor de Servicios.

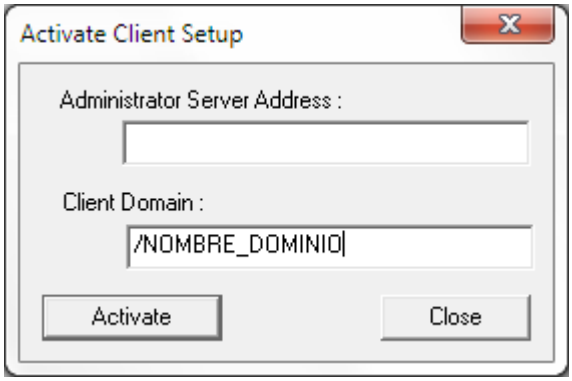


Figura 24. Instalación de agente. Comprobaciones.

La activación de un cliente en un determinado servidor puede comprobarse de forma visual, es decir, comprobando que el cliente efectivamente aparece en la estructura jerárquica de dominios, dentro del menú "*Administration*" de la interfaz *Avamar Administrator*.

6.4.3.3 Ficheros de registro de agente

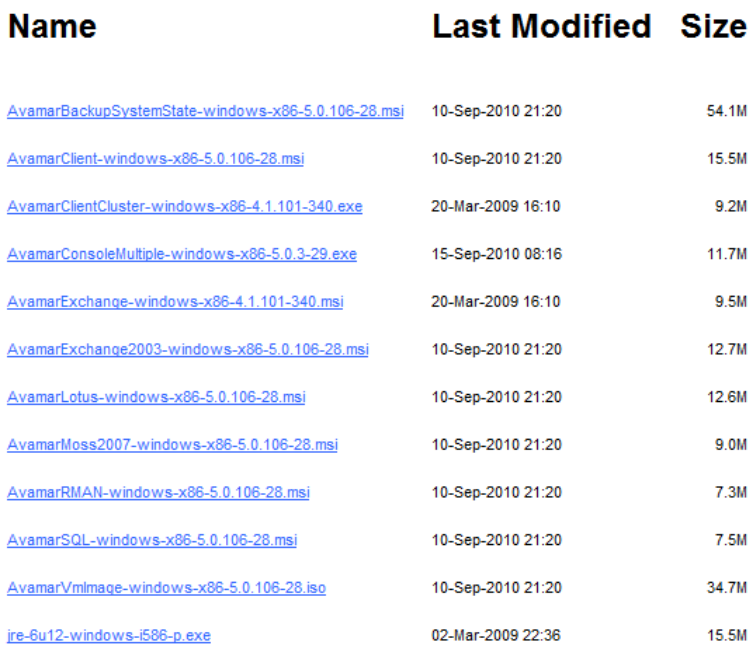
Puede que los administradores del servicio soliciten el siguiente fichero de registro ante una incidencia:

- Windows : C:\Program Files\avs\var\avagent.log
- UNIX: /opt/AVMRclnt/var/avagent.log

6.4.4 Instalación de la consola de Avamar

Para tener acceso a la consola de administración de Avamar, es necesario descargar e instalar el software desde la web que publica el servicio para distribuir documentación y software.

Para ello, hay que apuntar un navegador a la dirección http://backupenlanube.proveedordeservicios.org y seleccionar el enlace *Documents and Downloads* que conducirá página de descargas:



Name	Last Modified	Size
AvamarBackupSystemState-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	54.1M
AvamarClient-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	15.5M
AvamarClientCluster-windows-x86-4.1.101-340.exe	20-Mar-2009 16:10	9.2M
AvamarConsoleMultiple-windows-x86-5.0.3-29.exe	15-Sep-2010 08:16	11.7M
AvamarExchange-windows-x86-4.1.101-340.msi	20-Mar-2009 16:10	9.5M
AvamarExchange2003-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	12.7M
AvamarLotus-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	12.6M
AvamarMoss2007-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	9.0M
AvamarRMAN-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	7.3M
AvamarSQL-windows-x86-5.0.106-28.msi	10-Sep-2010 21:20	7.5M
AvamarVmImage-windows-x86-5.0.106-28.iso	10-Sep-2010 21:20	34.7M
jre-6u12-windows-i586-p.exe	02-Mar-2009 22:36	15.5M

Figura 25. Selección de plataforma de Consola.

Si el servidor donde se va a instalar la consola no tiene instalada la versión 6 o superior de Java, es necesario descargar e instalar el fichero *jre-6u12-windows-i586-p.exe*.

Para instalar la consola de Avamar, hay que descargar e instalar el fichero "*AvamarConsoleMultiple-windows.exe*". El asistente guía la instalación.

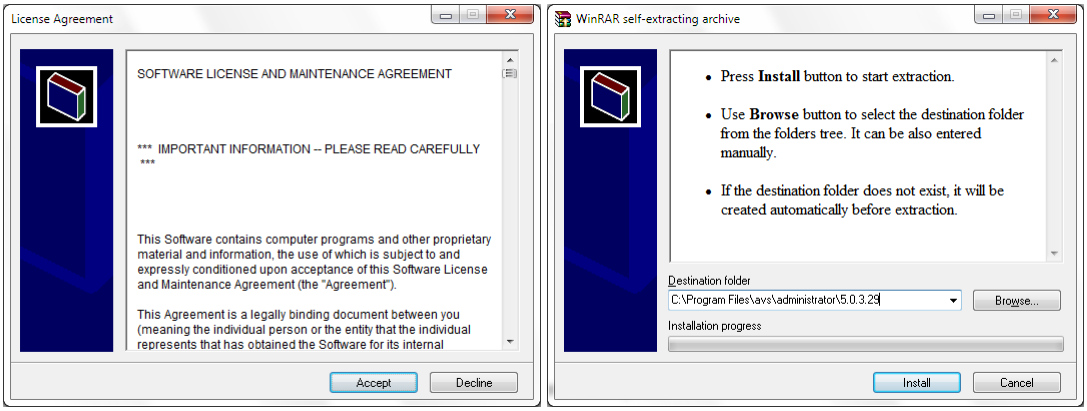


Figura 26. Instalación de consola.

El asistente copiará los ficheros necesarios.

6.4.5 Conexión al dominio de cliente

El acceso al dominio de cliente se realiza desde la consola de Avamar, para ejecutar la consola, desde el menú inicio, navegar por programas, EMC Avamar, Administrator y ejecutar Avamar Administrator.

Aparecerá la siguiente ventana:

Figura 27. Pantalla de bienvenida. Consola de Avamar.

Si es la primera ejecución de la consola, es conveniente configurar el servidor por defecto para no tener que rellenar esa información en cada acceso.

Para ello, pinchar en el botón "*Options*" y modificar los siguientes parámetros:

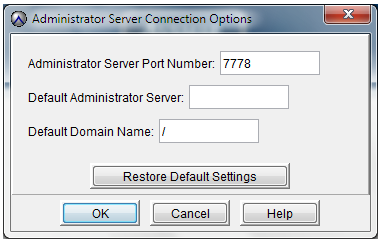


Figura 28. Opciones de Conexión. Consola Avamar.

- *Default Administrator Server*: backupenlanube.proveedordeservicios.org
- *Default Domain Name*: nombre de dominio proporcionado por el Proveedor de Servicios. El nombre de dominio contendrá el nombre del cliente y tendrá como máximo 20 caracteres.

El primer acceso al dominio se realizará con el usuario *admin* proporcionado por el Proveedor de Servicios (así como la contraseña).

La ventana principal de la consola de administración de Avamar consiste en un menú con las opciones de *Actions*, *Tools*, *Navigation* and *Help*. Así como seis botones etiquetados como *Policy*, *Backup & Restore*, *Administration*, *Backup Management*, y *Activity*.

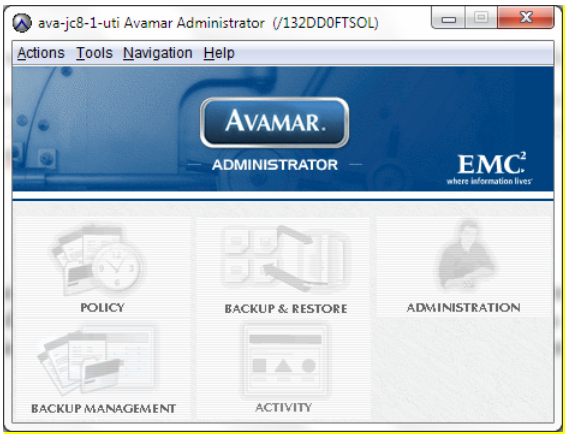


Figura 29. Consola de Administración.

En la Consola de Administración de Avamar, la estructura del dominio se muestra en muchas de las vistas disponibles, en el panel de la izquierda. Haciendo clic en el recuadro situado más a la izquierda del árbol de dominios, se expande la estructura, mostrándose los subdominios (si es que existen) y grupos y clientes que hayan sido asignados a dicho dominio.

Si ya existen usuarios adicionales al usuario *admin*, los usuarios con roles *backup only operator*, *restore only operator*, *backup/restore operator*, *activity operator* pueden iniciar sesión en la consola de administrador de la misma forma que el usuario *admin*. Las funciones estarán limitadas a las descritas en el apartado 6.2.5.5.

6.4.6 Administración delegada

6.4.6.1 Dominio de cliente

Los dominios son zonas delimitadas dentro de Avamar, utilizadas para separar y organizar los distintos clientes de respaldo. Anidando unos dominios dentro de otros para crear una estructura, es posible crear una jerarquía para administrar organizaciones y los clientes en esas organizaciones.

La creación de subdominios está limitada a usuarios *superadministradores* del sistema, por tanto, si se desea utilizar subdominios, se deberá solicitar la creación del subdominio correspondiente vía solicitud al grupo de administradores del sistema, facilitando los siguientes datos:

- Numero de contrato.
- Ruta del subdominio: por ejemplo, /CLIENTE/subdominio1

6.4.6.2 Usuarios de dominio

Se podrán crear hasta un máximo de diez usuarios dentro del dominio, con independencia de si existen subdominios, es decir, la suma de los usuarios creados en el dominio padre de un cliente y sus subdominios no puede llegar a más de diez.

Sólo existirá un usuario administrador del dominio, el resto de usuarios (hasta nueve) tendrán cualquiera de los roles descritos en el apartado 6.2.5.5.

6.4.6.3 Creación, edición y borrado de usuarios

Como ya se ha comentado anteriormente, el máximo número de usuarios de un dominio está limitado a diez, incluyendo el usuario por defecto *admin* (administrador del dominio).

Para crear un nuevo usuario, desde la ventana *Administration* se deberá seleccionar *Actions, Account Management, New User* o bien, haciendo clic con el botón derecho en el dominio/subdominio adecuado.

Los atributos que deberán especificarse son:

- Sistema de Autenticación: el sistema de autenticación es un sistema de nombre y contraseña usado para poder acceder al servidor de Avamar. El servicio contempla el sistema de autenticación nativo de Avamar, *Axion Authentication System*. El resto de sistemas de autenticación no están soportados en esta versión del servicio.

- Nombre de usuario: el nombre de usuario es sensible a mayúsculas y minúsculas.
- Rol: el servicio soporta los cuatro roles de usuarios.
- Contraseña. necesaria para garantizar la autenticación de los distintos usuarios.

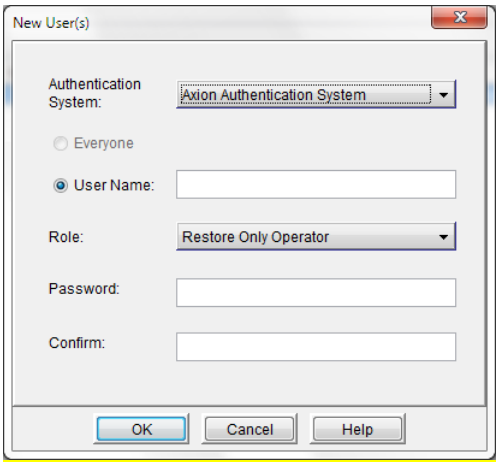
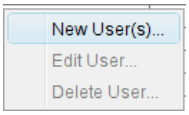


Figura 30. Creación de usuarios. Consola de Avamar.

Una vez creado el usuario, éste podrá ser borrado o editado, para modificar alguno de sus atributos. Haciendo clic con el botón derecho en el usuario y seleccionando *Edit User* o *Delete User*.



6.4.7 Configuración de recursos

En este apartado se van a describir todos los recursos necesarios para la planificación de copias de respaldo, es decir, iniciadas desde el servidor de manera automática. Se va a describir cómo crear los recursos, cómo modificarlos y cómo eliminarlos. Los recursos necesarios para este propósito son grupos, conjuntos de datos, políticas de retención y calendarios.

La consola de DPA puede tardar horas en refrescar el árbol con los objetos creados en Avamar.

6.4.7.1 Grupos

Un grupo en Avamar incluye uno o más clientes. También contiene una Política de Grupo, constituida por un conjunto de datos, un calendario y una política de retención que determinan cómo el grupo controla el comportamiento del respaldo. Los respaldos son programados mediante la configuración y activación de grupos; cuando el grupo se ejecuta, se hace copia de los clientes que son miembros de dicho grupo, de acuerdo con las especificaciones de la Política de Grupos.

El usuario *admin* (con permisos de administrador de dominio) puede configurar políticas de respaldo persistentes, seleccionando de qué quiere hacerse respaldo y cuándo quiere hacerse, mediante la creación, modificación o borrado de conjuntos de datos, calendarios y políticas de retención, asignándolos a un nuevo grupo o a uno previamente existente, y por último, añadiendo clientes a dicho grupo.

Para ver los grupos, organizados por dominios, habrá que seleccionar la pestaña *Groups* dentro de la vista *Policy* y el nivel de la jerarquía que quiere ser analizado. Un listado de los grupos incluidos en el dominio seleccionado se muestra en el panel de la derecha. Marcando la casilla *Show sub-domain groups*, todos los grupos incluidos en los subdominios, además de los grupos del propio dominio son mostrados.

Los grupos se crean dentro de la estructura de dominio definida. Cuando se crea un nuevo grupo, se debe especificar el conjunto de datos, calendario y política de retención que utilizará ese grupo.

Para crear un nuevo grupo, hay que seleccionar la pestaña *Groups* dentro de la vista *Policy*, *Policy Management*. En esta pestaña, se hará clic con el botón derecho en el nivel de la jerarquía donde se desee crear el nuevo grupo y se seleccionará *New Group*. Otra alternativa será marcar el nivel de la jerarquía en el que se quiere crear el nuevo grupo y hacer clic en *Actions, New Group*.

Los atributos mostrados en la primera ventana del *New Group wizard* son:

- *Name*: nombre del grupo. No se deben usar caracteres especiales o espacios.
- *Disabled*: Por defecto, el grupo se crea deshabilitado. Éste debe ser habilitado para que se ejecuten los respaldos de forma automática. Para habilitar un grupo que actualmente se encuentra deshabilitado, habrá que desmarcar la casilla *Disabled*, o dentro de la pestaña *Groups* de la vista *Policy*, seleccionar el grupo y a continuación seleccionar *Actions > Group > Disable Group*.
- *Encryption method*: se dejará la opción por defecto.
- *Override Schedule*: está opción se marca para sobrescribir el calendario asignado al grupo. La opción *Skip Next Backup* se seleccionará para no ejecutar el próximo respaldo planificado; mientras que la opción *Run Next Backup Once,* se selecciona para ejecutar el próximo respaldo planificado una única vez.

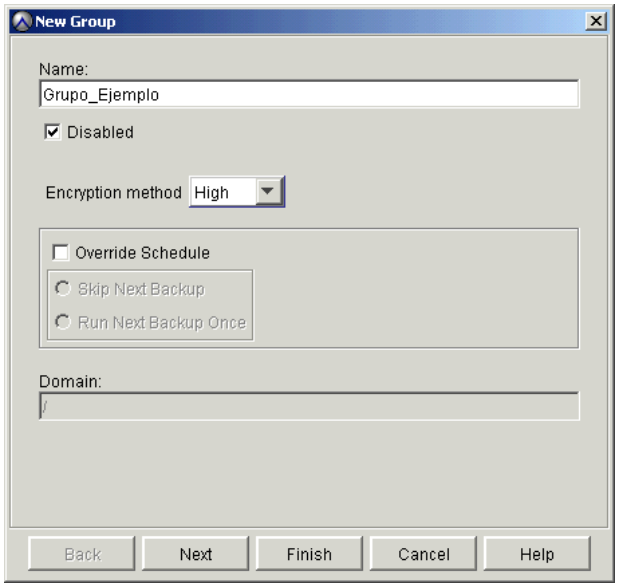


Figura 31. Creación de nuevos Grupos.

En las siguientes ventanas, deberá seleccionarse un conjunto de datos, un calendario y una política de retención previamente existentes. Los elementos que se muestran son aquellos que han sido creados en el mismo dominio o en un nivel superior en la jerarquía que el grupo que se está creando.

Durante la creación de un grupo, los conjuntos de datos, calendarios o políticas de retención no podrán ser modificados. Sin embargo, las propiedades de los mismos se mostrarán de forma que el administrador podrá analizarlas antes de hacer una selección.

Por último, habrá que seleccionar los clientes que van a ser miembros de este grupo. Los clientes deben haber sido activados en el mismo dominio que el grupo, o bien en un subdominio del dominio en el cuál se está creando el grupo.

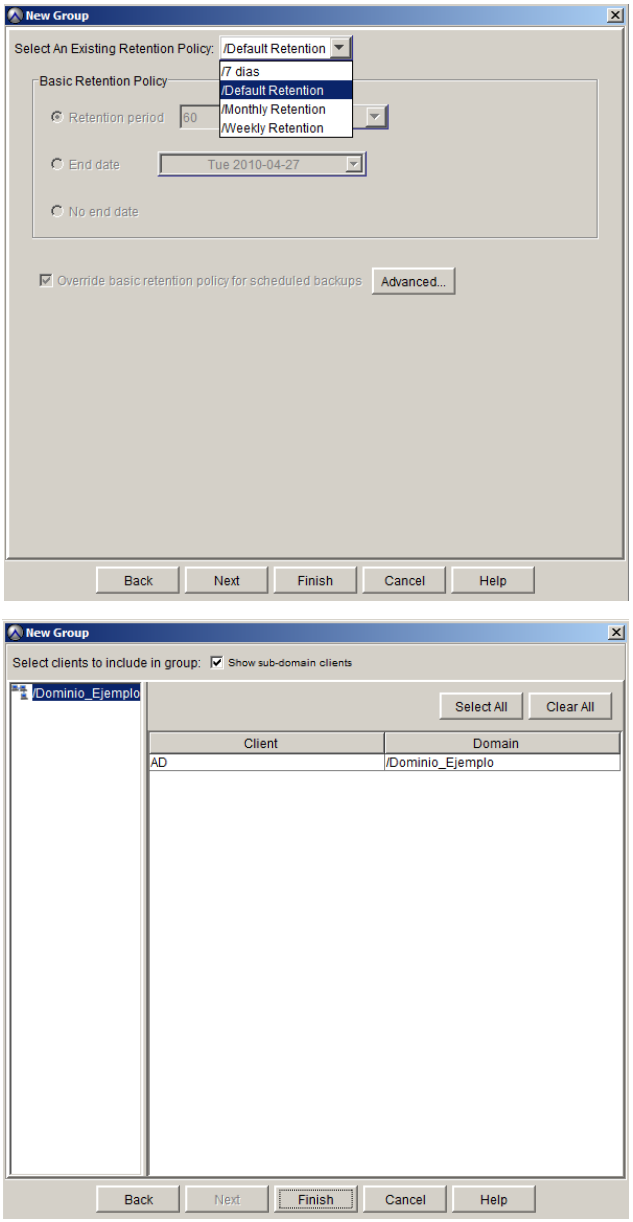


Figura 32. Creación de Grupos. Selección de Usuarios.

Los clientes heredan las especificaciones configuradas en la Política de Grupo, es decir, el conjunto de grupos, el calendario y la política de retención del grupo del que forman parte. Las especificaciones del conjunto de datos y la política de retención pueden sobrescribirse haciendo asignaciones específicas cliente por cliente. Sin embargo, los calendarios pueden aplicarse únicamente a grupos y no a clientes específicos.

Para sobrescribir la Política de Grupo en un determinado cliente debe seleccionarse la pestaña *Clients* dentro de la vista *Policy*, *Policy Management*, seleccionar el cliente que se quiera modificar del panel derecho y hacer click en *Edit*. En la ventana que aparece se pueden modificar tanto los atributos seleccionados durante la creación del cliente, como la Política de Grupo, es decir, el conjunto de datos y la política de retención.

Para ello en la pestaña *Dataset* o *Retention Policy* del cliente seleccionar la casilla de *Override* para priorizar el conjunto de datos o retención seleccionada a nivel de cliente frente a la seleccionada a nivel de grupo:

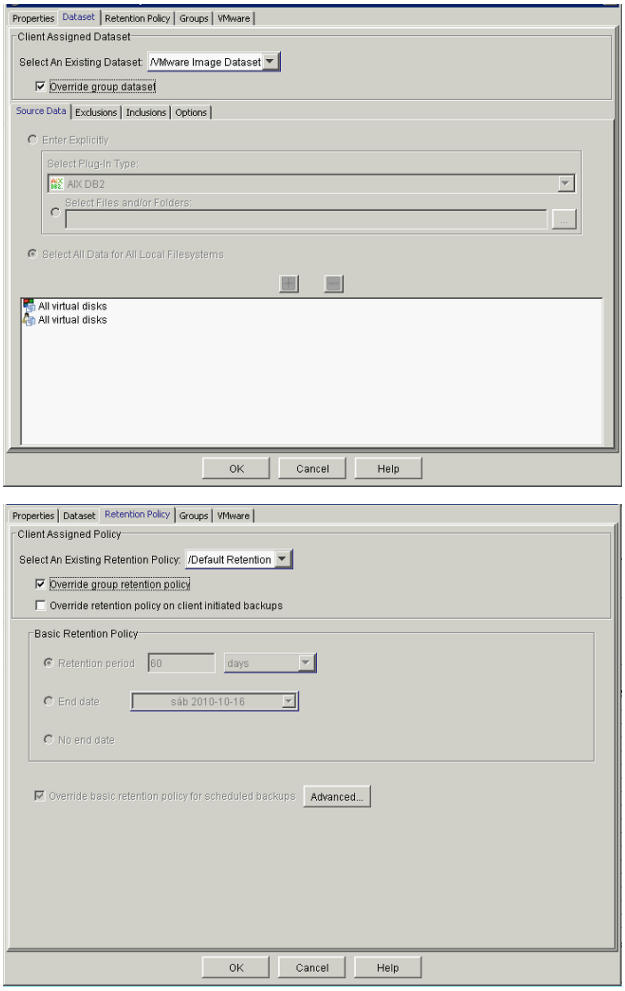


Figura 33. Modificación de Propiedades de Grupos.

Una vez creados, los grupos pueden ser modificados, es decir, se puede cambiar el nombre del grupo, el conjunto de datos, el calendario, la política de retención y los clientes asignados a dicho grupo. Asimismo, un grupo puede ser copiado o eliminado. Para llevar a cabo estas acciones es necesario situarse en la pestaña *Groups* de la vista *Policy*, *Policy Management* y seleccionar la acción deseada.

También es posible mostrar un informe en el que se muestra una vista rápida de los conjuntos de datos, calendarios, políticas de retención y clientes de todos los grupos presentes en el sistema. Para ver dicho informe es necesario seleccionar la pestaña *Group Summary Reports* dentro de la vista *Policy*. Para ver la información relativa a la Política de Grupo, será necesario pinchar en la pestaña correspondiente (*Datasets*, *Calendarios*, *Políticas de retención*, *Clientes*). En la figura se muestra la pestaña *Schedules*, por ejemplo:

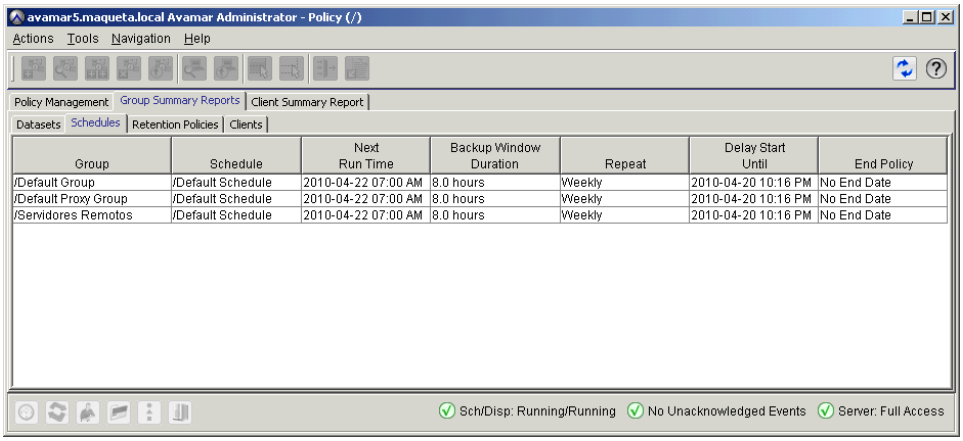


Figura 34. Informe de Agendas.

6.4.7.2 Conjuntos de Datos

Los conjuntos de datos definen los sistemas de ficheros, directorios o ficheros seleccionados para ser incluidos en un respaldo. Los conjuntos de datos se pueden crear en cualquier nivel de dominio y pueden ser asignados a uno o más clientes y grupos dentro del respectivo dominio/subdominios.

Avamar proporciona varios conjuntos de datos pre configurados en el dominio *root*, lo que implica que pueden ser utilizados por cualquier grupo o cliente en toda la jerarquía:

- *Default Dataset*: Hace respaldo de todos los sistemas de ficheros locales. Por defecto, este conjunto de datos es asignado al *Default Group*. La utilización de este conjunto de datos asegura que todos los clientes del grupo están haciendo respaldo de todos sus datos sin importar el sistema operativo en el que estén corriendo.
- *Base Dataset*: Define un conjunto de requisitos mínimos. Esencialmente se trata de un conjunto de datos vacío.
- *Unix and Windows Datasets*: Están optimizados para ser utilizados con los respectivos tipos de clientes.

En la definición de un conjunto de datos se puede incluir más de un tipo de complemento. Avamar utilizará el adecuado en cada respaldo, basándose en el tipo de cliente del que se esté haciendo respaldo y/o complemento instalado en el cliente. En muchos casos, se va a utilizar el conjunto de datos pre configurado, el *Default DataSet*, para hacer respaldo de todos los sistemas de ficheros locales en todos los clientes. Sin embargo, habrá clientes en los que sea necesaria la creación de un nuevo conjunto de datos para la definición de requerimientos específicos de forma persistente.

Para crear un nuevo conjunto de datos, se seleccionará *Tools > Manage Datasets*. A continuación, se seleccionará el nivel deseado dentro de la estructura de dominios en el cual se quiere utilizar el nuevo conjunto de datos y se hará *click* en *New*.

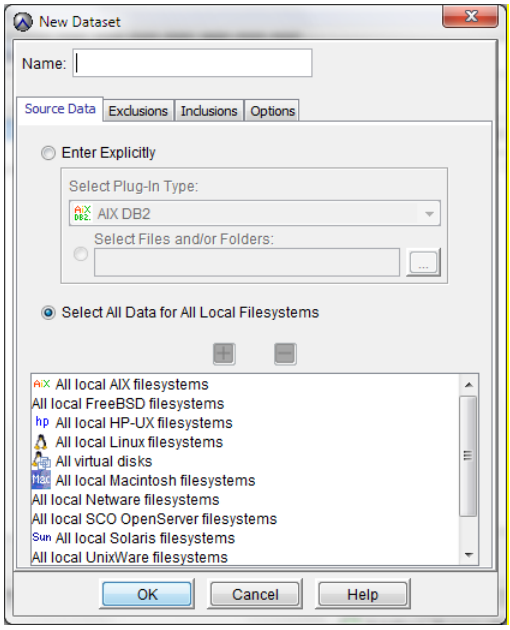


Figura 35. Creación de conjuntos de datos.

Cada conjunto de datos define de qué datos se va a hacer respaldo, inclusiones, exclusiones y opciones. Habrá de tenerse en cuenta que en el nombre dado al nuevo conjunto de datos no podrán utilizarse ni caracteres especiales ni espacios.

En la pestaña *Source*, se seleccionarán los datos de los cuales se va a hacer respaldo mediante esta instancia de conjunto de datos. Habrá que decidir si se quieren seleccionar todos los datos de sistemas de ficheros locales o por el contrario, si se quiere especificar de qué sistemas de ficheros en concreto se quiere hacer respaldo. Si se introducen objetos de forma explícita, la entrada por defecto "*All local filesystems*" es eliminada.

En las siguientes figuras se muestran dos conjuntos de datos con dos especificaciones de datos distintas. En la primera de ellas se han seleccionado todos los sistemas de ficheros Linux, mientras que en la segunda de ellas se ha especificado de manera explícita el directorio F:\ de un sistema de ficheros Windows.

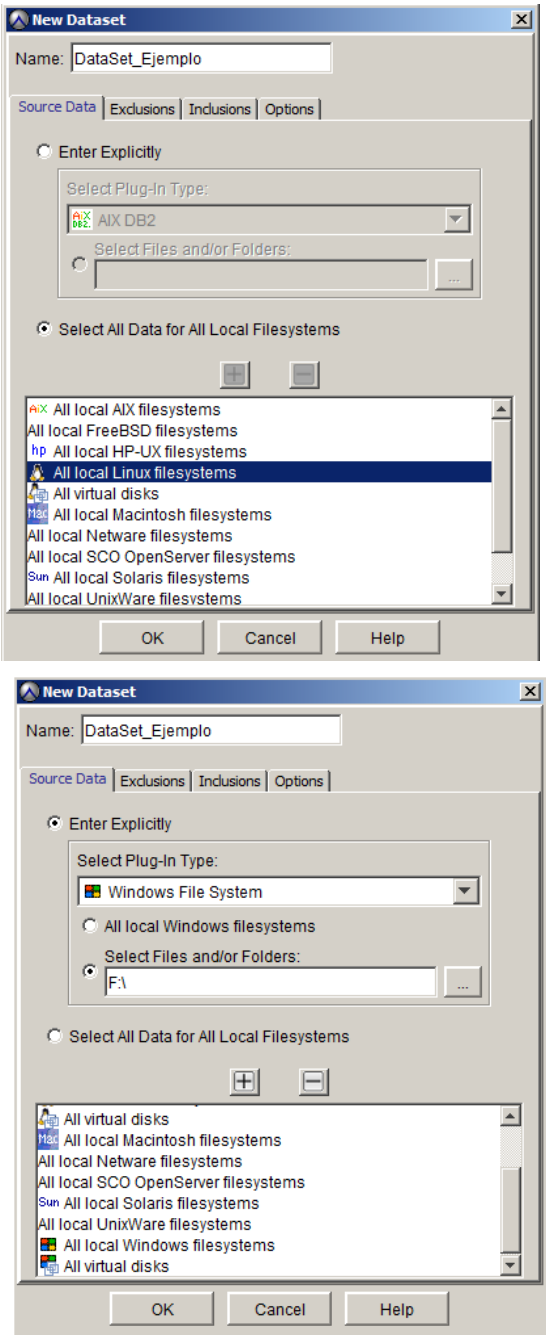


Figura 36. Configuración de nuevos Conjuntos de Datos.

En la pestaña *Exclusions*, se especificarán los directorios o ficheros que se quieren excluir de la selección hecha en la pestaña *Source Data*. En la figura que se muestra a continuación, se están excluyendo todos los ficheros con extensión ".jpg". Ha de tenerse en cuenta que hay una serie de ficheros que son excluidos del respaldo de forma automática, como ocurre, por ejemplo con los ficheros de caché locales de Avamar.

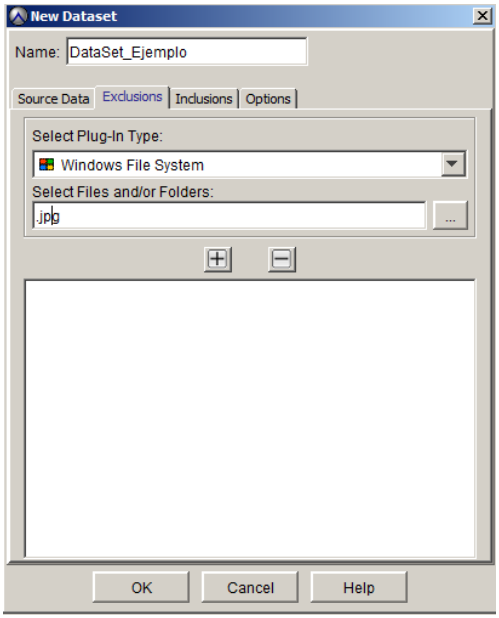


Figura 37. Ejemplo de exclusión.

La pestaña *Inclusions*, se utiliza para incluir ficheros determinados que han sido excluidos en la lista de exclusión especificada en la pestaña anterior. En la figura que se muestra a continuación, se incluye en el respaldo el fichero "Ejemplo.jpg", el cual había sido excluido en la regla anterior, dónde se excluían todos los ficheros con extensión "jpg".

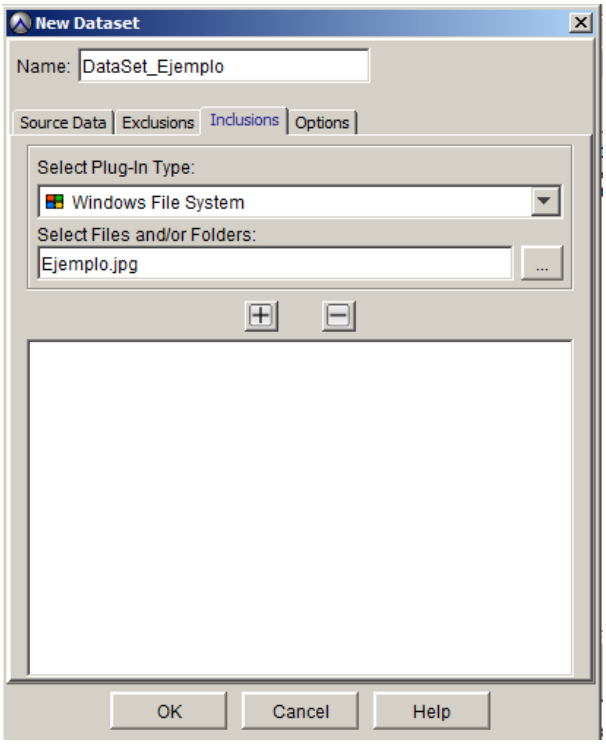


Figura 38. Ejemplo de inclusión.

Haciendo *click* en la pestaña *Options* y seleccionando un determinado complemento, se muestran todas las opciones disponibles para dicho complemento. Un único conjunto de datos puede incluir opciones que atañan a más de un tipo de

complemento, ya que como se ha comentado anteriormente, un conjunto de datos puede incluir más de un tipo de datos.

Las figuras que se muestran a continuación presentan algunas de las opciones disponibles para el complemento *Windows Filesystem*. Las opciones pueden seleccionarse directamente en la interfaz de usuario o, por el contrario, se pueden insertar como valores de texto. Por ejemplo, una etiqueta puede ser añadida al respaldo, proporcionando un valor al atributo *Backup Label*, como se muestra en la primera de las siguientes figuras. La otra alternativa sería insertar el atributo *label* en el campo *Enter Attribute* y un valor para dicha etiqueta en el campo *Enter Attribute Value*. A continuación, sería necesario seleccionar el signo "+" para añadir la opción a la lista de opciones del complemento seleccionado.

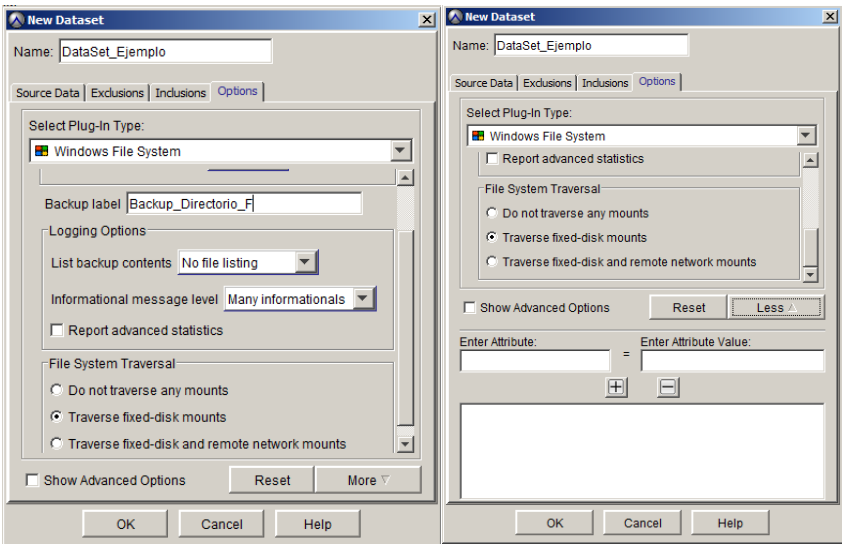


Figura 39. Opciones del complemento Windows Filesystem.

Haciendo *click* en *Show Advanced Options* se muestra una lista de opciones, las cuales son interesantes si se está haciendo detección de problemas o ajustando el sistema. Por ejemplo, si se está intentando solucionar un problema en un determinado respaldo, sería interesante activar el modo de depuración durante un cierto período de tiempo. También pueden incluirse scripts que se ejecutarán antes o después del respaldo, mediante las opciones de *Pre-Script* y *Post-Script*.

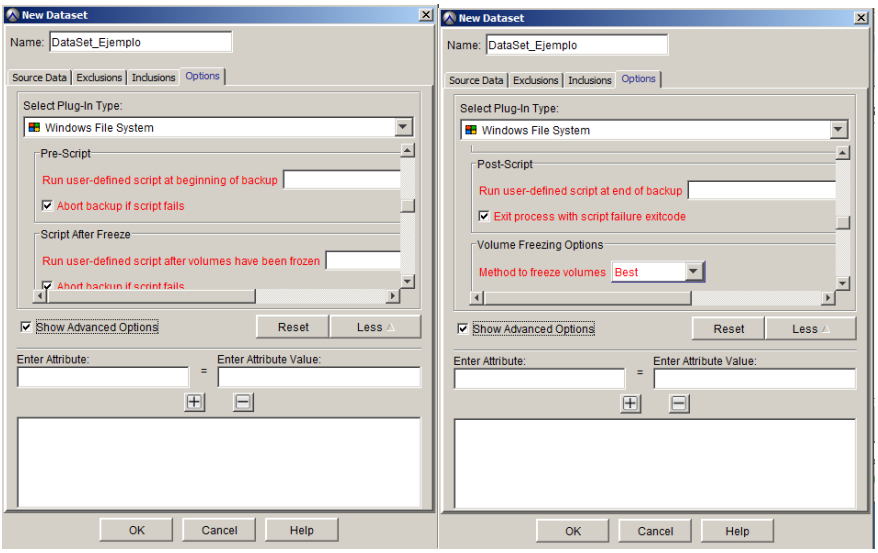


Figura 40. Configuración avanzada de Conjuntos de Datos.

Los conjuntos de datos pueden ser modificados, es decir, se puede cambiar el nombre, la lista de exclusiones e inclusiones y las opciones seleccionadas para cada tipo de datos. Asimismo, un conjunto de datos puede ser copiado o eliminado. Para llevar a cabo estas acciones es necesario situarse en la vista *Tools* > *Manage DataSets* y seleccionar la acción deseada.

6.4.7.3 Políticas de Retención

Las retenciones especifican cuánto tiempo se va a guardar un determinado respaldo. Todo respaldo con una antigüedad superior a la especificada es automáticamente dado de baja en el sistema.

Las políticas de retención se pueden crear en cualquier nivel de dominio y pueden ser asignados a uno o más clientes y grupos dentro del respectivo dominio/subdominio.

Al igual que ocurre con los grupos y los conjuntos de datos, Avamar proporciona una serie de políticas de retención pre configuradas:

- *Default Retention*: retención de 60 días.
- *Monthly Retention*: retención de un mes.
- *Weekly Retention*: retención de una semana.

Para crear una nueva política de retención, hay que seleccionar *Tools* > *Manage Retention Policies*. A continuación, seleccionar el nivel deseado en la estructura de dominios y hacer clic en New. En Avamar hay dos tipos de políticas de retención, las políticas de retención básicas y las políticas avanzadas.

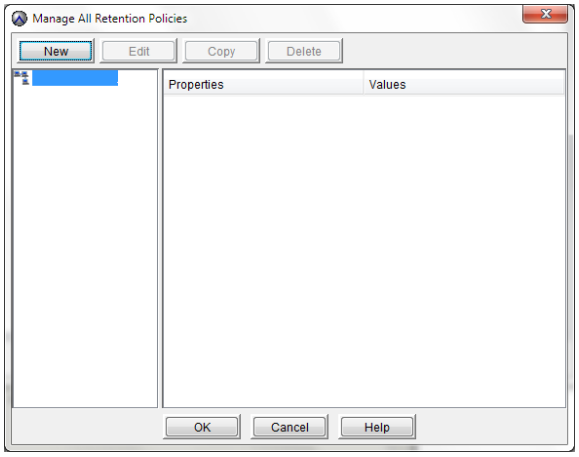


Figura 41. Creación de nueva Política de Retención.

Para configurar una política de retención básica, además de incluir el nombre de la política (en el cual no se podrán utilizar ni espacios ni caracteres especiales) habrá que seleccionar una de las siguientes opciones:

- *Retention period*: Período de retención fijo ligado al momento en el que se inicia el respaldo, expresado en días, semanas, meses o años.
- *End date*: Asigna una fecha del calendario como fecha de expiración.
- *No end date*: Esta opción es utilizada cuando se quiere retener un respaldo de forma indefinida. Los respaldos con esta política son retenidos tanto tiempo como el cliente esté activo en el servidor de Avamar.

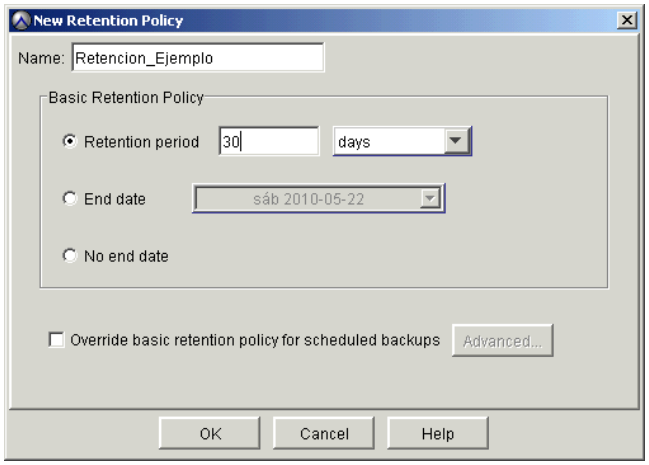


Figura 42. Configuración de Política de Retención.

Las políticas de retención avanzadas son utilizadas con respaldos de ejecución diaria, para asignar una política de retención de forma dinámica, dependiendo de cuánto tiempo quieran retenerse los respaldos diarios, semanales, mensuales y anuales en el sistema. Estas retenciones están ligadas al momento en el que se inicia el respaldo.

El primer respaldo que se ejecuta de forma satisfactoria cada día es considerado el respaldo diario; de igual forma el primer respaldo que se ejecuta de forma satisfactoria cada semana es considerado el respaldo semanal. Lo mismo ocurre con los respaldos mensuales y anuales. Hay que tener en cuenta que cada semana comienza el domingo, a

partir de medianoche 00:00:01 GMT. Cada mes comienza después de la media noche del primer día del mes y cada año comienza después de medianoche del día uno de enero.

Para crear una política de retención avanzada, es necesario seleccionar la opción *Override basic retention policy for scheduled backups*, mientras se crea una política de retención básica. A continuación, deberá hacerse clic en *Advanced*. A partir de ahí se deberá rellenar todas las especificaciones necesarias para completar la política de retención avanzada. En el ejemplo mostrado a continuación se ha asignado una retención de treinta días para los respaldos diarios, de ocho semanas para los respaldos semanales, de seis meses para los respaldos mensuales y de dos años para los respaldos anuales.

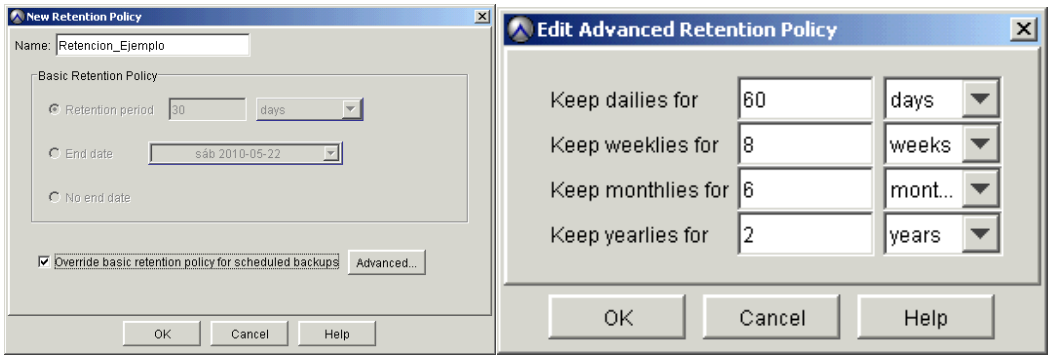


Figura 43. Edición de Políticas de Retención..

Una vez creadas, las políticas de retención pueden ser modificadas, es decir, se puede cambiar el nombre de la política y las retenciones. Asimismo, una política de retención puede ser copiada o eliminada. Para llevar a cabo estas acciones es necesario situarse en la vista *Tools > Manage Retention Policies* y seleccionar la acción deseada.

6.4.7.4 Calendarios

Los calendarios determinan cuándo y con qué frecuencia se ejecuta un respaldo. Se pueden crear en cualquier nivel de la jerarquía de dominios y pueden ser asignados a uno o más grupos dentro del respectivo dominio/subdominios.

Para crear un nuevo calendario, hay que situarse en *Tools > Manage Schedules*, posicionarse en el nivel deseado de la jerarquía y hacer clic en New.

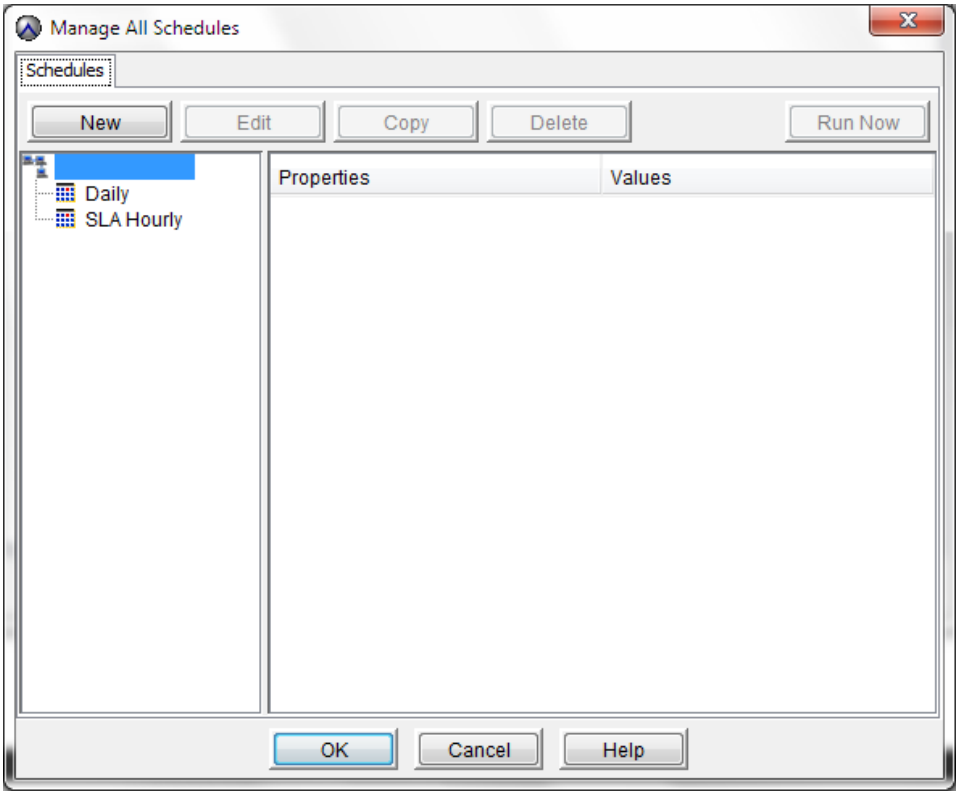


Figura 44.Creación de nuevo Calendario.

Durante la creación de un calendario se definen las siguientes características:

- Repetición (*Repetition*): La repetición indica con qué frecuencia es ejecutado el calendario. Las opciones incluidas son: *Daily*, *Weekly*, *Monthly* and *On-Demand*, es decir, diario, semanal, mensual y bajo demanda. Los calendario bajo demanda no se ejecutan nunca; este tipo de calendario suelen asociarse a grupos que son ejecutados manualmente.
- Horario de Operación (*Operating hours*): Este parámetro especifica la ventana de tiempo durante la cual el respaldo puede ser ejecutado.
- Si se selecciona la opción *Daily*, se deberá seleccionar al menos una hora del día en las que se ejecutarán los respaldos. Deberá especificarse también la duración máxima de los mismos.
- Si se selecciona la opción *Weekly* o *Monthly*, se deberá especificar la hora a la que los respaldos pueden comenzar, al igual que la en la que el respaldo es abortado por el servidor de Avamar si no ha terminado.
- Limitaciones de activación (*Activation Constraints*): Este parámetro especifica el período de tiempo durante el cual el calendario será aplicado. Puede especificarse que se ejecute para siempre, seleccionando el parámetro *No End Date* o, por el contrario, puede especificarse una fecha a partir de la cual no se quiere ejecutar más el respaldo, marcando la opción *End After*.

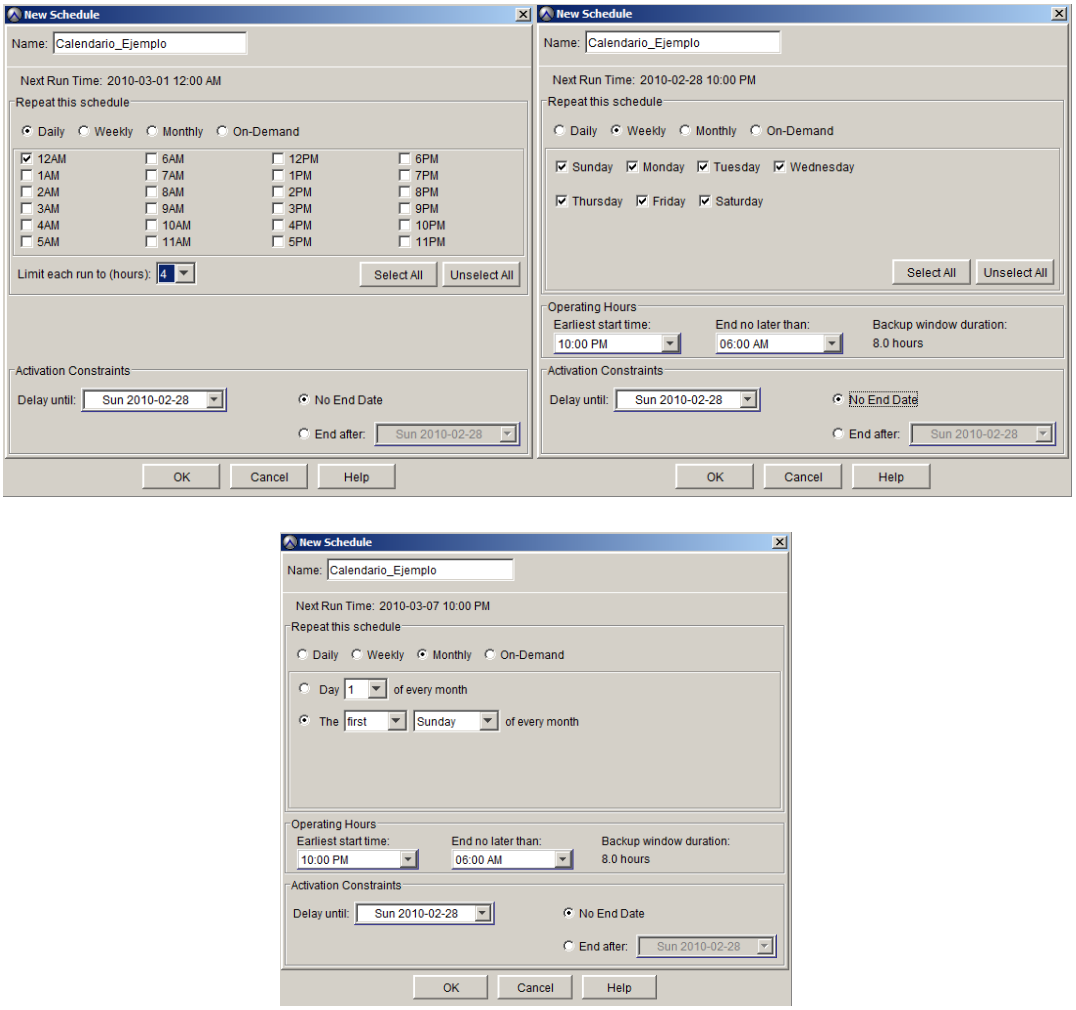


Figura 45.Configuración de nuevos Calendarios.

Los tiempos que se muestran cuando se crea o se edita un calendario, así como los tiempos mostrados en la mayoría de las vistas de la Consola de Administración, están basados en la zona horaria local donde el administrador está creando la sesión con la Consolas.

A la hora de crear calendarios hay que tener en cuenta varias consideraciones. El calendario pre configurado se ejecuta cada noche, nunca antes de las 7 A.M. y terminando antes de las 3 P.M. Esto significa que ningún respaldo con este calendario se va a ejecutar antes de las 7 A.M. y que a las 3 P.M. se terminará toda actividad de respaldo que se ejecute con este calendario. Si un respaldo se sale de ventana, el sistema lo parará, recordará lo que ha salvado hasta ahora y al día siguiente continuará el trabajo en el punto en que se quedó. Este comportamiento se controla mediante el parámetro *Operating hours* documentado en la página anterior.

Avamar ejecuta diariamente varios procesos de mantenimiento que empiezan a las 8 A.M. y terminan a las 4 P.M. como muy tarde. A la ejecución de estas tareas de mantenimiento se las conoce como '*Daily Maintenance Schedule'* y para que se ejecuten de manera eficiente es extremadamente importante que ningún respaldo se ejecute en esa ventana de tiempos.

La ventana de respaldo de *Default Schedule* está configurada de tal manera que no interfiera con las tareas de mantenimiento diarias.

Al configurar nuevos calendarios, es necesario tener en cuenta el apartado de Ventanas de Operación de este documento, ya que durante la ventana de mantenimiento no se pueden ejecutar respaldos.

Una vez creados, los calendarios pueden ser modificados, es decir, se puede cambiar el nombre del mismo, la frecuencia de lanzamiento, los horarios y todos los demás parámetros. Asimismo, un calendario puede ser copiado o eliminado.

Los calendarios, además, presentan algunas opciones específicas:

- *Suspend All*: Esta opción se utiliza para deshabilitar todos los respaldos planificados.
- *Resume All*: Esta opción habilitará los respaldos planificados.
- *Run Now*: Se utiliza para activar de forma inmediata todas las acciones asociadas con el calendario seleccionado.

Para llevar a cabo estas acciones es necesario situarse en la vista *Tools* > *Manage Schedules* y seleccionar la acción deseada.

6.4.7.5 Ventanas de operación

Avamar ejecuta diariamente varios procesos de mantenimiento que empiezan a las 8 A.M. y terminan a las 4 P.M. como muy tarde. A la ejecución de estas tareas de mantenimiento se las conoce como '*Daily Maintenance Schedule'* y para que se ejecuten de manera eficiente es extremadamente importante que ningún respaldo se ejecute en esa ventana de tiempos.

Si se inicia un respaldo bajo demanda o si se programa un respaldo para que se inicie muy próximo a las 8 a.m. (por ejemplo 7 a.m.) y el respaldo no ha terminado a las 8 a.m. cuando comienza la ventana de mantenimiento, el sistema cancelará el trabajo para que pueda comenzar la ventana de mantenimiento.

Igualmente, si se lanza un respaldo bajo demanda o si se programa un respaldo para que se inicie durante la ventana de mantenimiento, el sistema lo cancelará automáticamente y aparecerá en la consola de actividad como fallido.

Estos trabajos cancelados volverán a ejecutarse al día siguiente normalmente, sin embargo, la información salvada el día que el respaldo se cancelo es válida y no se enviara de nuevo, con lo cual al día siguiente esa información no se volverá a enviar.

Cuando el sistema está fuera de la ventana de mantenimiento, el número de hilos de respaldo y restauración de la plataforma tiene un límite, y al tratarse de una plataforma compartida, puede que los trabajos no comiencen exactamente a la hora programada y se encolen si se ha superado el número máximo de hilos del sistema.

6.4.8 Respaldo y Restauración

6.4.8.1 Respaldo

El servicio ofrece dos tipos de respaldos: el planificado y el bajo demanda. Los respaldos planificados se ejecutan automáticamente de acuerdo con los parámetros especificados durante la configuración. Se lanzarán de acuerdo con el calendario asignado al grupo al que pertenezca el cliente y se hará respaldo de los datos especificados en el conjunto de datos correspondiente.

Los respaldos bajo demanda se iniciarán desde la consola Avamar. El respaldo desde la consola de cliente no está soportado.

6.4.8.1.1 Respaldo planificado

El respaldo planificado se configura a través de grupos utilizando conjuntos de datos, calendarios y políticas de retención según se indica en el apartado 6.4.7 Configuración de recursos.

6.4.8.1.2 Respaldo bajo demanda

Los respaldos bajo demanda se ejecutan desde la vista "*Backup and Restore*". Seleccionando en el árbol de la izquierda el cliente del que se quiere hacer respaldo y, en la pestaña "*Select for Backup*", se seleccionarán los sistemas de ficheros, ficheros y directorios que quieran salvarse. A continuación se seleccionará *Actions* > *Back Up Now*.

En la ventana "*On Demand Backup Options*" se pueden especificar la retención del respaldo así como las siguientes opciones avanzadas:

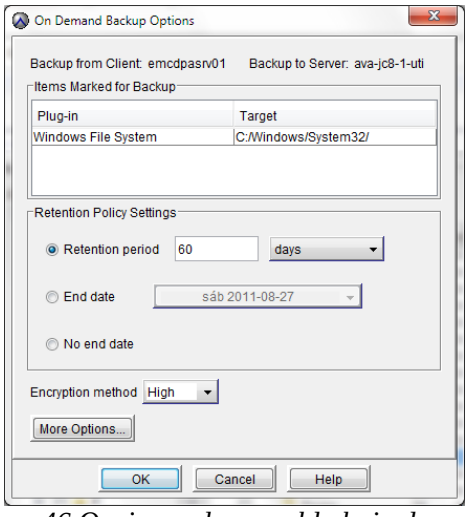


Figura 46.Opciones de respaldo bajo demanda.

Otra opción disponible sería lanzar un grupo completo bajo demanda a través de la vista *Policy*, *Policy Management*, pestaña *Groups*, seleccionando el grupo y haciendo clic en "*Back up*". Existe la misma opción a nivel de cliente desde la pestaña *Clients*, seleccionando el cliente y haciendo *click* en "*Back up*". A continuación, en la ventana "*Select Group for Client Backup*" se seleccionará un grupo de entre los que el cliente sea

miembro. Los conjuntos de datos de los que se hará respaldo serán aquellos definidos en el conjunto de datos del grupo seleccionado.

6.4.8.2 Restauración

El servicio sólo soporta la opción de restauración desde la consola de administración de Avamar.

Para realizar una restauración, desde la vista "*Backup and Restore*":

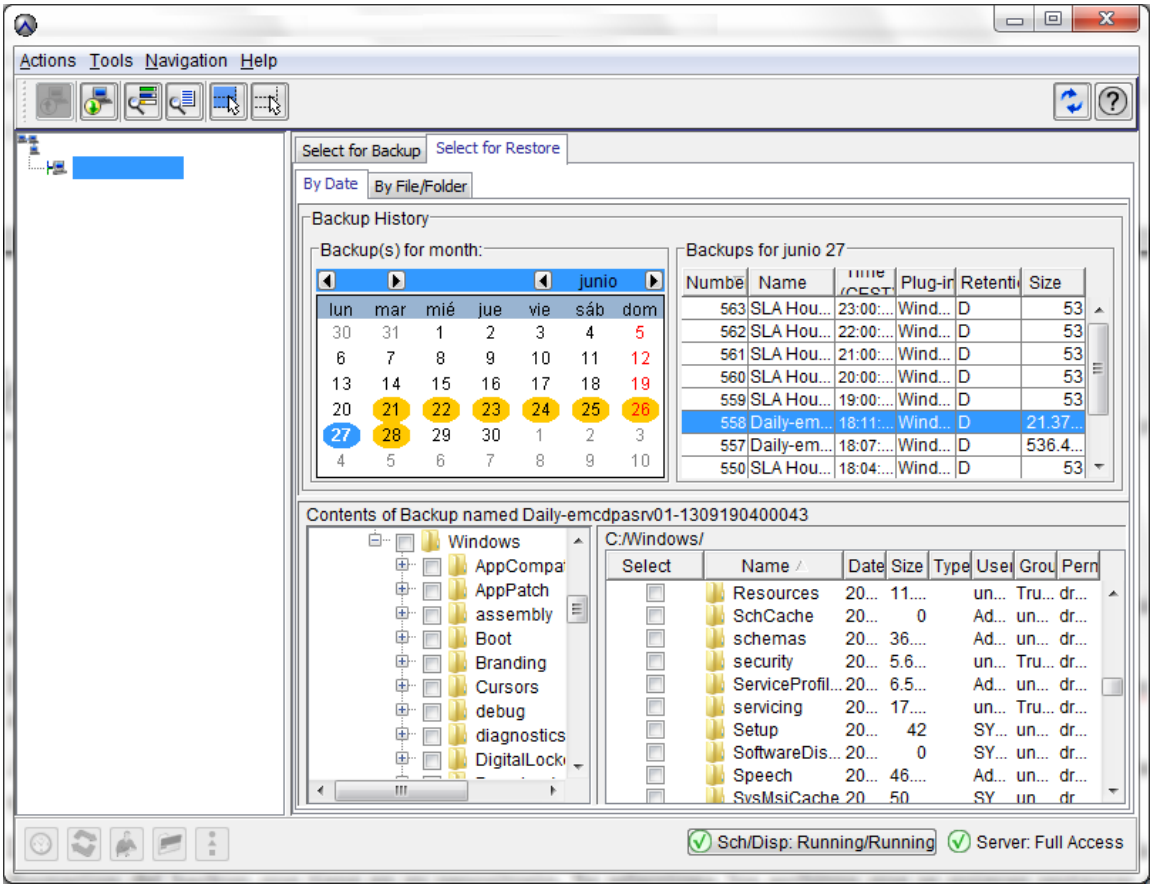


Figura 47.Restauración de copia de respaldo.

1. Se selecciona la pestaña "*Select for restore*" y en árbol de la izquierda, se elige el cliente del cual se quieren recuperar los datos.
2. En la sección "*Backups for month*" se selecciona la fecha del respaldo que se quiere restaurar. Los días que aparecen en amarillo indican que existe una copia de respaldo válida para ese cliente.
3. A la derecha de la seccion "*Backups for month*" está la sección "*Backups for day*" que muestra los respaldos que existen para ese día.
4. La parte inferior muestra el árbol de directorios que lee Avamar del índice que ha creado a partir de la información del respaldo que tiene en su repositorio. Se selecciona los archivos que se quieran restaurar desde el nivel de directorios deseado (por ejemplo, la letra de unidad "C", un directorio, o incluso, el cliente completo)
5. Desde el menú "*Actions"*, se selecciona "*Restore Now"* para verificar las opciones y comenzar la actividad.

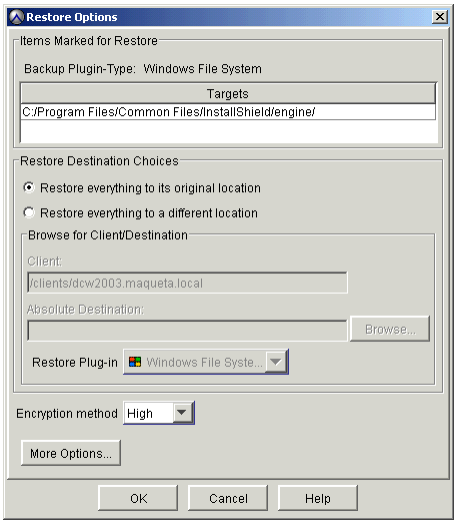


Figura 48.Opciones de restauración de copia de respaldo.

Existen dos opciones principales:

1. "*Restore everything to its original location"*: restaura los ficheros a la ubicación original.
2. *"Restore everything to a different location*": permite restaurar a una ubicación diferente, incluido otro cliente de Avamar.

6.4.9 Monitorización de trabajos

Toda la monitorización de trabajos en ejecución se realiza desde la vista "A*ctivity*" de la consola Avamar Administrator. Para llegar a ella:

1. Se inicia la consola de administración de Avamar. Dependiendo del rol del usuario que se autentique en la consola, tendrá visibilidad de más o menos eventos dentro de la vista de *Activity*.
2. El usuario *admin* tiene visibilidad de todos los eventos del dominio. Un usuario con rol de *restore only operator* sólo tiene visibilidad de los trabajos de restauración que haya iniciado el mismo.
3. Desde el menú inicial, se hace clic en la opción *Activity*.
4. Seleccionar la pestaña *Activity Monitor*.

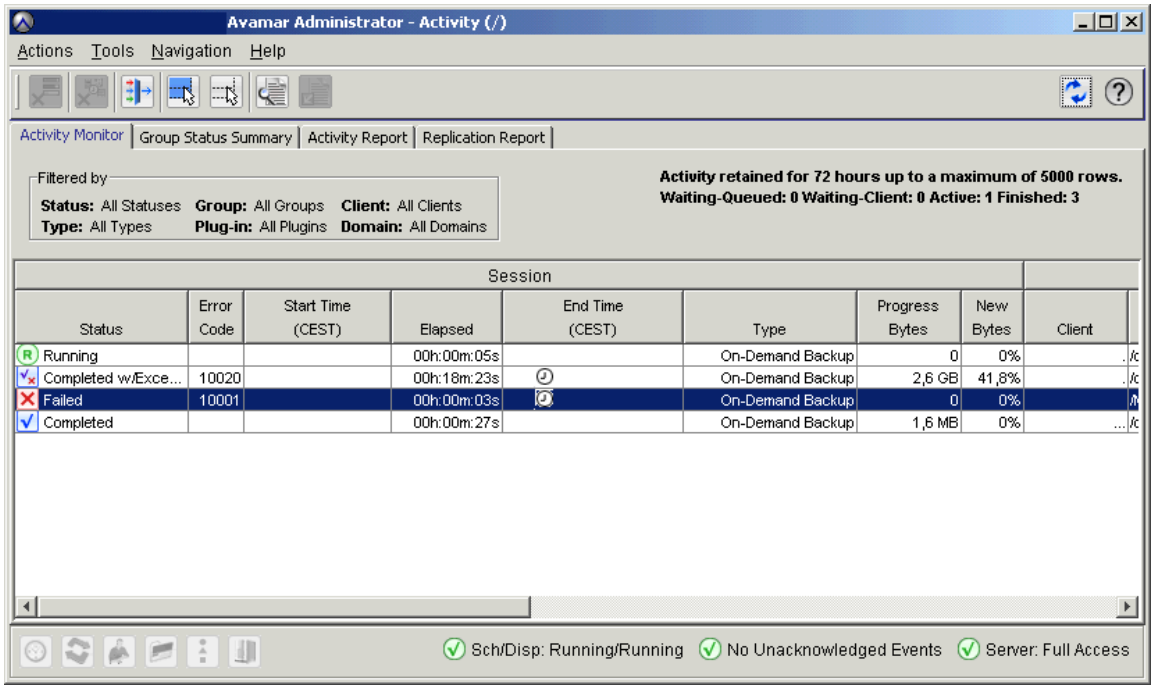


Figura 49.Opciones de respaldo bajo demanda.

La ventana muestra la actividad de las últimas 72 horas (o los últimos 5000 trabajos). La siguiente tabla muestra el significado de las distintas columnas y valores:

COLUMNA	DESCRIPCIÓN
Status	***!Checkin*** El trabajo no puede comenzar porque el cliente no estaba disponible cuando el servidor tenía recursos disponibles. Ocurre si un cliente se desconecta de la red. La actividad permanece encolada y puede pasar a estado Activo cuando el cliente conecta con el servidor. ***!Started*** Actividad fallida el empezar. ***Canceled*** El trabajo fue cancelado por el cliente o por el Administrador. ***Client Backup Disabled*** La opción de comenzar respaldos desde este cliente ha sido desactivada. ***Complete*** Actividad completada con éxito. ***Disconnected*** Actividad terminada debido a la falta de respuesta del cliente. ***Dropped Session*** Actividad iniciada correctamente pero debido a la falta de Actividad, es forzada por el Administrador a estado deshabilitado. ***Failed*** El cliente falló al ejecutar la actividad, finalizando en una condición de error. ***Finished w Exception(s)*** Actividad completada con errores menores o advertencias. Es necesario contactar con el administrador de sistemas para revisar el registro de errores. ***No Status*** El trabajo no está progresando y el servidor de Avamar no puede determinar su estado. ***Restore Disabled*** Las operaciones de restauración han sido deshabilitadas para este cliente.

Status	***Running*** Cliente en ejecución. ***Scheduled Backup Disabled*** Las operaciones de respaldo planificados han sido deshabilitadas para este cliente. ***Stalled*** El trabajo no está progresando como era de esperar. Dado que el servidor no puede proveer el estado del mismo, el problema se localiza en el cliente. ***Suspended*** El trabajo ha sido suspendido. ***Undefined*** El trabajo no tiene una orden de trabajo asociada. ***Unknown*** El trabajo ha generado un código de salida desconocido desde el cliente. ***Validate Disabled*** Todas las operaciones de validación de respaldo han sido deshabilitadas para este cliente. ***Waiting for Client*** El trabajo está esperando que el cliente conecte con el servidor de Avamar, con el fin de que pueda comenzar la misma. ***Waiting, backlogged*** Actividad en espera, pendiente disponibilidad cliente/servidor.
Error Code	Si la actividad no fue completada satisfactoriamente un código de error. Es necesario contactar con el Administrador del servicio para revisar el registro de errores.
Start Time	Hora en que la actividad fue iniciada.
Elapsed/End Time	Si la actividad está en ejecución el tiempo de actividad de la misma Si la actividad ha finalizado, tiempo de ejecución y hora de finalización.
Type	La actividad es del tipo siguiente: On-Demand Backup Scheduled Backup Restore Validate Replication Source Replication Destination
Dataset Name	Nombre del conjunto de datos empleado en esta actividad.
Progress Bytes	Número de Bytes analizados durante esta actividad.
New Bytes	Porcentaje de Nuevos Bytes enviados al servidor de Avamar (Bajos números indican altos niveles de Deduplicación).
Client Name	Nombre del cliente en la configuración de Avamar.
Domain	Dominio de Avamar.
OS	Sistema Operativo del Cliente.

Client Release	Versión del cliente instalado.
Group	Grupo al que pertenece el cliente dentro de una actividad planificada.
Plug-in	Complemento empleado para esta actividad.
Current Retention	Retención actual del cliente.
Original Retention	Retención original en la planificación de este conjunto de datos.
Schedule	Calendario asociado a esta actividad.
WID	Identificador de la orden de trabajo que identifica de manera unívoca a la actividad (*Work Order Id*)

Tabla 4.Significado de las columnas de Monitorización de Trabajos.

6.5 Consideraciones de Seguridad del Servicio

6.5.1 Autenticación de usuario y Autorización

1. Cambiar las contraseñas por defecto de los usuarios de sistema (*root, MCUser, admin, replonly, dpn*) tras la primera instalación del sistema.
2. No usar información personal a la hora de crear las contraseñas (nombre, nombre de usuario, fechas relevantes, nombres de familiares).
3. Cambiar las contraseñas cada 6 meses como máximo.
4. Nunca compartir las contraseñas, especialmente por teléfono.

6.5.2 Control de Acceso por Red

1. Todos los clientes deben ser capaces de conectarse a todos los servidores de Avamar y viceversa.
2. Es necesario un servidor de DNS y resolución directa e inversa de nombres para todos los nodos.
3. El acceso al servicio se efectuará vía VPN, a no ser que sea absolutamente imposible para el cliente, en cuyo caso el cliente deberá proveer sus propias medidas de seguridad para su entorno.
4. Tanto los clientes como los servidores del Servicio de Respaldo en la nube utilizan Seguridad en la Capa de Transporte (*TLS*) e Infraestructura de Clave Pública (*PKI*) para la autenticación y el encriptado de los datos en tránsito.
5. El sistema utilizará autenticación de dos vías entre clientes y servidores.
6. Como medida de seguridad adicional para los accesos al servicio que se hagan vía Internet sin utilización de VPN, se implementará Lista de Control de Acceso (*ACLs*) en los switches dedicados de acceso, permitiéndose únicamente la conexión al servicio a las IPs que sean proporcionadas por el cliente como

habilitadas para el uso. Se implementará asimismo un Cortafuegos que examine el tráfico de red y permita el paso únicamente de las tramas de red que pertenezcan al servicio de Respaldo en la Nube.

6.5.3 Seguridad e Integridad de los Datos

1. Los datos transferidos entre clientes y servidores del servicio siempre viajarán encriptados (certificados X.509) con una intensidad de 128 bits.
2. Además de viajar encriptados, los nodos de almacenamiento también salvaguardarán los datos, cifrándolos mediante AES 128 CFB (*Cipher Feedback*).
3. Para asegurar la integridad de los datos, Avamar guardará puntos de control (*checkpoints)* con el único fin de prevenir su pérdida o inconsistencia. Estos puntos de control son validados tras ser hechos (2 veces al día por el sistema o bajo demanda), y en caso de pasar este control, se consideran válidos para una reversión o "*rollback*" del sistema en caso de ser necesario.
4. Las copias de respaldo expiradas o borradas manualmente, por defecto, no son eliminadas inmediatamente de disco, sino que son marcadas como borradas. Los datos no serán sobrescritos a no ser que sea necesario el espacio, o se solicite específicamente por medio de petición a los Administradores del Servicio.

6.5.4 Auditoría, Registro y Monitorización del Sistema

1. El sistema monitorizará y guardará registro de todas las actividades de respaldo y restauración, así como de otras actividades administrativas realizadas por parte de los usuarios. Los datos almacenados incluirán tipo de actividad, estado, horas de inicio y fin, severidad de la acción, dominio en el que se ha realizado, código de error (si aplica), así como otros datos de interés acerca de la actividad.
2. También se monitorizará el estado de los componentes fundamentales del sistema, como el estado general, capacidad, estado de los nodos y sus particiones, creación de puntos de control y demás actividades de mantenimiento.
3. Los administradores del servicio tendrán acceso a las alertas generadas por el sistema tanto por correo electrónico como por envío de *Traps* SNMP a la herramienta de recolección de alertas puesta a disposición.

6.5.5 Bastionado de nodos del sistema

Se ha optado por un bastionado compatible con STIG Nivel 1 (*Security Technical Implementation Guide*) para todos los nodos no clientes del servicio. Las medidas de seguridad adoptadas son las siguientes:

1. Entorno de detección de intrusos avanzado (AIDE - *Advanced Intrusion Detection Environment*).
2. Servicio de Auditado (*auditd*) – Se audita el servidor, por si se realiza algún cambio que comprometa su capacidad de actuar según sus especificaciones.

3. Implantación de *sudo* – Habilita a los usuarios *dpn* y *admin* (a nivel de sistema operativo) a ejecutar comandos que requerirían privilegios del usuario *root*. De esta manera se elimina la necesidad de habilitar acceso como usuario *root*.
4. Registro de ejecución de comandos – Los sistemas registrarán todos los ejecutados por todos y cada uno de los usuarios.
5. Deshabilitar Samba.
6. Eliminar la opción de cifrado débil de Apache.
7. Forzar cifrado de 128 bits o superior a las conexiones Java (Apache y Tomcat).
8. Eliminar el bit de suid de los binarios de sistema no esenciales.
9. Prevenir el acceso no autorizado a la configuración de GRUB (gestor de arranque).

6.5.6 Lista de Comprobaciones de Requisitos LOPD

6.5.6.1 Nivel aplicable al Servicio

A la hora de definir el servicio se ha de determinar el nivel de seguridad LOPD aplicable al mismo, para lo cual se deberá rellenar la columna de la derecha de la tabla con SI (se tratan datos de esta tipología) o NO (no se tratan este tipo de datos). Al final del documento se asignará el el nivel aplicable al servicio basándonos en dicha tabla, la cual está creada teniéndo en cuenta las consideraciones establecidas en el punto 5.6 del presente documento.

NOTA: Por normativa interna del Proveedor de Servicios, incluso aquellos proyectos o servicios que no incluyen ningún tipo de dato de carácter personal deberán cumplir las estipulaciones del nivel BÁSICO de la LOPD.

ID	DATOS	APLICABLE
1	NOMBRE Y APELLIDOS	**SI**
2	DIRECCIÓN (postal, electrónica, IP)	**SI**
3	FIRMA/ HUELLA DIGITALIZADA	NO
4	Nº SS – MUTUALIDAD	NO
5	MARCAS FÍSICAS	NO
6	AFILIACIÓN SINDICAL	NO
7	CREENCIAS	NO
8	SALUD	NO
9	DATOS DE ESTADO CIVIL	NO
10	FECHA DE NACIMIENTO	NO
11	EDAD	NO
12	NACIONALIDAD	NO
13	CARACTERÍSTICAS FÍSICAS O ANTROPOMÉTRICAS	NO
14	SITUACIÓN MILITAR	NO
15	AFICIONES Y ESTILO DE VIDA	NO
16	LICENCIAS, PERMISOS, AUTORIZACIONES…	NO
17	HISTORIAL DEL ESTUDIANTE	NO

18	PERTENENCIA A COLEGIOS Y ASOCIACIONES DE PROFESIONALES	NO
19	PUESTO DE TRABAJO	NO
20	HISTORIAL DEL TRABAJADOR	NO
21	CREACIONES ARTÍSTICAS, LITERARIAS, CIENTÍFICAS O TÉCNICAS	NO
22	LICENCIAS COMERCIALES	NO
23	INVERSIONES, BIENES PATRIMONIALES	NO
24	DATOS BANCARIOS	NO
25	DATOS ECONÓMICOS DE NÓMINA	NO
26	SEGUROS	NO
27	SUBSIDIOS, BENEFICIOS	NO
28	TARJETAS DE CRÉDITO	NO
29	BIENES Y SERVICIOS RECIBIDOS POR EL AFECTADO	NO
30	COMPENSACIONES / INDEMNIZACIONES	NO
31	DNI- NIF	**SI**
32	TELÉFONO	**SI**
33	FIRMA ELECTRÓNICA	NO
34	IMAGEN / VOZ	NO
35	IDEOLOGÍA	NO
36	RELIGIÓN	NO
37	ORIGEN RACIAL O ÉTNICO	NO
38	VIDA SEXUAL	NO
39	DATOS DE FAMILIA	NO
40	LUGAR DE NACIMIENTO	NO
41	SEXO	NO
42	LENGUA MATERNA	NO
43	CARACTERÍSTICAS DE ALOJAMIENTO, VIVIENDA	NO
44	PROPIEDADES, POSESIONES	NO
45	PERTENENCIA A CLUBES, ASOCIACIONES…	NO
46	FORMACIÓN, TITULACIONES	NO
47	EXPERIENCIA PROFESIONAL	NO
48	PROFESIÓN	NO
49	DATOS NO ECONÓMICOS DE NÓMINA	NO
50	ACTIVIDADES Y NEGOCIO	NO
51	SUSCRIPCIÓN A PUBLICACIONES / MEDIOS DE COMUNICACIÓN	NO
52	INGRESOS – RENTAS	NO
53	CRÉDITOS, PRESTAMOS, AVALES	NO
54	PLANES DE PENSIONES, JUBILACIÓN	NO
55	DATOS DEDUCCIONES IMPOSITIVAS / IMPUESTOS	NO
56	HIPOTECAS	NO
57	HISTORIAL CRÉDITOS	NO
58	BIENES Y SERVICIOS SUMINISTRADOS POR EL AFECTADO	NO
59	TRANSACCIONES FINANCIERAS	NO

Tabla 5.Cálculo de Nivel LOPD.

NIVEL APLICABLE AL SERVICIO	**BÁSICO**

6.5.6.2 Comprobaciones de Seguridad Aplicables al Servicio

MEDIDA	REALIZADO	COMENTARIOS
DOCUMENTACIÓN		
La Oferta Tipo y el Contrato del Servicio (si se genera) deben especificar dos cosas: • El nivel de LOPD que es capaz de cubrir el servicio. • La obligación del cliente de no introducir datos de un nivel superior de LOPD en el sistema. •	SI	Se indicará nivel **Básico**.
Si en el desarrollo del servicio es preciso utilizar un software específico se debe incluir en el contrato del desarrollo, o de la utilización de dicho software, la indicación explícita del nivel de LOPD que dicho software debe cumplir.	SI	El software Avamar y su configuración para el proyecto cumplen con la LOPD nivel básico.
En la documentación del servicio (normalmente en el Manual de Usuario, y en el Manual de Operación) deben quedar especificados los diferentes actores en el servicio, los roles que tienen cada uno de ellos y la descripción de sus funciones y obligaciones. El software del servicio deberá ser coherente con los roles, funciones y obligaciones especificados.	SI	Lo que indica la LOPD en este apartado hace referencia a que todo el personal implicado en el proyecto que cuenta con datos de carácter personal deberá conocer exactamente cuál es su rol y que funciones y obligaciones implica éste de cara a preservar la privacidad de los datos. Para cumplir este requisito, generalmente se recurre a charlas de concienciación al personal. En el caso se ha acordado sustituir esa concienciación por la especificación, dentro de la documentación del servicio de todas las personas o grupos (roles) que intervienen en el servicio, en un modo u otro, y que tienen acceso a los datos restringidos. Estos grupos incluyen tanto a personal del Proveedor de Servicios, personal subcontratado), como terceros (p.e. administraciones públicas intermediarias) y clientes.
Deberán reflejarse en el Protocolo de Mantenimiento los datos de carácter personal existentes en el Servicio, su ubicación, y especificar que son de nivel BASICO. En caso de que no se conozca a priori el detalle de los datos que se van a alojar, se debe indicar el nivel de LOPD definido y especificar que no se deberán alojar datos de nivel superior a ese.	SI	Se notificará por escrito al cliente durante la firma del contrato de servicio.

CONTROL DE ACCESO A LOS DATOS Y SISTEMAS		
Los accesos al software del servicio, así como a los sistemas de la plataforma, deberán cumplir los requisitos de identificación y autenticación definidos en el Protocolo de Gestión de Contraseñas del Proveedor de Servicio.	SI	Se forzará mediante políticas de usuario.
Si se precisa la existencia de grupos de administración específicos para el servicio, y éstos tienen acceso a los datos de carácter personal, para cada uno hay que informar: 1) Descripción de los diferentes perfiles del personal que lo conforma, junto con sus tareas. 2) Listado de las personas que lo conforman.	SI	No hay grupos de administración específicos, ya que la plataforma será gestionada por un grupo de administración ya existente.
Deberán guardarse los registros de accesos al sistema e incluir estos registros en la política de respaldo de la plataforma del servicio. Estos registros deberán conservarse al menos 1 año.	SI	A) Respaldo imagen diario de los servidores virtuales. La política establecida es: Diario: completo diario lo guarda 6 días Semanal: Imagen Semanal lo guarda una semana Mensual: guarda 12 meses B) Respaldo avanzado de las BBDD. La política establecida es: Diario: completo diario y diferencial cada 6 horas Semanal: Imagen Semanal lo guarda una semana Mensual: guarda 12 meses
GESTIÓN DE SOPORTES Y DOCUMENTOS		
Si en el Servicio se definen documentos o soportes informáticos (CDs, DVDs, cintas, etc.) que contengan datos de carácter personal y que no vayan a ser tratados por los procedimientos estándar de la casa (respaldo, librarian, etc.), se debe especificar el procedimiento para su tratamiento.	NO APLICA	
RESPALDO Y RESTAURACIÓN		
La política de respaldo debe establecer una copia total de datos al menos una vez por semana.	SI	A) Respaldo imagen diario de los servidores virtuales. La política establecida es: Diario: completo diario lo guarda 6 días Semanal: Imagen Semanal lo guarda una semana Mensual: guarda 12 meses B) Respaldo avanzado de las BBDD. La política establecida es: Diario: completo diario y diferencial cada 6 horas Semanal: Imagen Semanal lo guarda una semana Mensual: guarda 12 meses

PRUEBAS DE SISTEMA		
Las pruebas de software del servicio previas al paso a Explotación deberán hacerse con datos ficticios. Si es necesario utilizar datos reales, hay que hacer respaldo previo y registrar las pruebas.	SI	Las pruebas unitarias, de integración y de certificación se han hecho con datos ficticios.
MEDIDAS EN FASE DE EXPLOTACIÓN		
Ante una incidencia de seguridad que afecte a la información de carácter personal incluida en el servicio, hay que rellenar una 'Plantilla de Incidentes de Seguridad'.	SI SI	En el caso de que se contemple en el servicio la existencia de posibles incidentes de seguridad que afecten a la información almacenada, la operativa a seguir es la siguiente: 1.- Rellenar plantilla Incidentes de Seguridad. 2.- Abrir incidencia al Grupo de Seguridad de la Información. Subtipo de incidencia INCIDENTE DE SEGURIDAD. Adjuntar la plantilla de incidentes.
Cuando haya que proceder al borrado de un soporte informático con datos de carácter personal, deberá comunicarlo al responsable de los datos y dejar registrada la actuación.	SI	En caso de que el servicio que se está definiendo contemple la existencia de documentos o de otros soportes que incluyan información sometida a LOPD, que vayan a manejarse de forma ajena a los procesos estándar del Proveedor de Servicios deberán especificarse los procesos de manipulación de esa información, con los responsables de ejecutarlo, de autorizarlo, etc.: Responsable que autoriza la manipulación de los datos. Responsable de ejecutar la manipulación de los datos. Descripción del proceso de manipulación de los datos.
En caso de que se lleven a cabo pruebas con datos reales durante la explotación del Servicio, hay que hacer respaldo previo y registrar las pruebas. En todo caso, se procurará efectuar estas pruebas con datos ficticios.	NO APLICA	
Deberá llevar a cabo pruebas semestrales de recuperación de los datos de carácter personal contenidos en el Servicio, y registrar dichas pruebas.	SI	Para cada prueba de respaldo deberá rellenarse un registro con los siguientes datos: • Política de Respaldo Actualizada • Funcionamiento de los respaldos. • Nº respaldos fallidos frente a número de respaldos total. • ¿Ha sido necesario utilizar el

Deberá llevar a cabo pruebas semestrales de recuperación de los datos de carácter personal contenidos en el Servicio, y registrar dichas pruebas.	SI	procedimiento de recuperación de datos? • Recuperación de datos a través de copia de respaldo. • ¿Se han recuperado datos manualmente? • ¿Se ha perdido algún tipo de información?
Si se produce una pérdida de datos de carácter personal en el proceso de respaldo o recuperación, deberá informarse la misma como un incidente de seguridad.	SI	Tratar igual que otros incidentes de seguridad descritos con anterioridad.
MEDIDAS EN FASE DE BAJA		
Cuando un cliente se dé de baja del servicio se deberá establecer con el cliente la operativa a realizar con los datos de carácter personal que obran en poder del Proveedor de Servicio dentro de la plataforma del servicio.	SI	Ante la baja de un cliente en el Servicio, el Responsable del Servicio en Explotación, junto con el Gestor de Producto, deberán acordar con dicho cliente el procedimiento de baja en lo relativo al tratamiento a realizar con los datos que dicho cliente tiene albergados en la plataforma del Servicio. El procedimiento acordado deberá cubrir los siguientes aspectos: • Cliente • Contrato • Fecha de baja • Fecha de comunicación del cliente • Periodo de retención • Cifrado de información • Fecha destrucción Hay que tener en cuenta las siguientes consideraciones: • El período de retención de los datos del cliente, posteriormente a su baja, nunca deberá ser inferior a un año. • El cliente es responsable de disponer de los medios necesarios para descifrar los datos, si opta por ese método. •
Cuando se proceda a la baja del servicio en el catálogo de la empresa cliente, se deberá dejar el correspondiente registro.	SI	El Gestor de Producto junto con el Responsable del Servicio deberán rellenar los siguientes datos una vez que se haya dictaminado dar de baja el servicio del catálogo: • Fecha de alta del servicio • Proveedores implicados • Fecha de baja del servicio • Devolución de información por proveedor

		• Fecha de comunicación a clientes Además, para cada cliente existente en el Servicio en el momento de la baja del mismo, deberá seguirse el procedimiento indicado para bajas de clientes.

Tabla 6.Consideraciones de Seguridad y Privacidad aplicables al servicio.

Capítulo 7

Presupuesto

7.1 Resumen de fases y línea temporal

A continuación se presenta de manera resumida y tabular las fases y subfases en las que se dividirá el proyecto de implación de la Plataforma de Respaldo en la Nube. Como resultado de la planificación, concluímos lo siguiente:

- Se comenzará con los trabajos previos el día 1 de Septiembre del 2015.
- El proyecto tendrá una duración total de 77 días.
- Dividiremos el proyecto en cinco grandes fases:
    - Arranque y organización – Durante esta fase se crea el equipo técnico responsable de la implantación, asi como la documentación inicial y se establecen los requisitos previos.
    - Diseño – Durante esta fase se diseña la solución de manera pormenorizada, generando la documentación de implantación.
    - Puesta en marcha – Instalación física de la solución, ejecución de tareas de puesta en marcha así como de pruebas de los entornos.
    - Puesta en Producción – Integración final con el resto de la infraestructura del Proveedor de Servicios. Realización de las primeras copias de respaldo con datos reales.
    - Documentación y cierre – Obtención de la aprobación del Proveedor de Servicios a la ejecución del Proyecto. Actualizaciones de última hora sobre la documentación del proyecto.

Nombre de la Tarea	Duración	Inicio	Finalización	Recursos
Plataforma de Respaldo en la Nube	**77 días**	**Mar 9/1/15**	**Mie 12/16/15**	
FASE 0 - Arranque y Organización	**9.5 días**	**Mar 9/1/15**	**Lun 9/14/15**	
Reunión de arranque interno de proyecto	1 día	Mar 9/1/15	Mar 9/1/15	PM,IS,SA
Creación del equipo de trabajo	4 hrs	Vie 9/4/15	Vie 9/4/15	PM
Reunión de arranque externo de proyecto	1 día	Vie 9/11/15	Lun 9/14/15	PM,IS,SA
Entrega del nuevo HW y licencias SW	0 días	Mar 9/1/15	Mar 9/1/15	
Fin fase 0	0 días	Lun 9/14/15	Lun 9/14/15	
FASE I - Diseño de la Solución	**19 días**	**Lun 9/21/15**	**Vie 10/16/15**	
Reunión de arranque técnico de diseño con cliente	1 día	Lun 9/21/15	Mar 9/22/15	PM,IS,SA
Entrega de documento pormenorizado de requisitos de instalación	4 hrs	Mie 9/23/15	Mie 9/23/15	SA
Elaboración del diseño y entrega del mismo	1 Sem	Mar 9/22/15	Mar 9/29/15	SA
Elaboración de los manuales de administración y operación de la plataforma	1 Sem	Mar 9/29/15	Mar 10/6/15	SA
Elaboración de los manuales de usuario	2 días	Mar 10/6/15	Jue 10/8/15	SA
Revisión del diseño y manuales con cliente, correcciones y aceptación	1 día	Jue 10/15/15	Vie 10/16/15	PM,IS,SA
Fin diseño global	0 días	Vie 10/16/15	Vie 10/16/15	
FASE II - Puesta en marcha de la solución	**29.5 días**	**Mie 10/7/15**	**Mie 11/18/15**	
Instalación de plataforma AVAMAR	**9.5 días**	**Mie 10/7/15**	**Mie 10/21/15**	
Fin de preparación de prerrequisitos de instalación HW	0 días	Mie 10/7/15	Mie 10/7/15	
Ubicación física del nuevo HW, conexión eléctrica y LAN de los equipos	1 día	Vie 10/16/15	Lun 10/19/15	PM,CE
Configuración inicial, instalación/actualización de versiones FW	1 día	Lun 10/19/15	Mar 10/20/15	IS
Integración de la solución con la Lunitorización y pruebas básicas de entorno	1 día	Mar 10/20/15	Mie 10/21/15	IS
Fin instalación plataforma AVAMAR	0 días	Mie 10/21/15	Mie 10/21/15	
Puesta en marcha plataforma DPE	**12.5 días**	**Mie 10/7/15**	**Lun 10/26/15**	
Fin de preparación de prerrequisitos de instalación SW	0 días	Mie 10/7/15	Mie 10/7/15	
Instalación del SW, configuración inicial	1 día	Vie 10/16/15	Lun 10/19/15	IS,SA
Preparación de los informes avanzados de acuerdo a la documentación de diseño y acuerdos con cliente	1 Sem	Lun 10/19/15	Lun 10/26/15	IS,SA
Fin instalación plataforma DPE	0 días	Lun 10/26/15	Lun 10/26/15	
Pruebas piloto de backup	**9 días**	**Lun 11/2/15**	**Vie 11/13/15**	
Pruebas de respaldo/restauración "remoto" via Internet	1 día	Lun 11/2/15	Mar 11/3/15	PM,IS,SA
Pruebas de respaldo/restauración "local" via VPN	1 día	Mar 11/3/15	Mie 11/4/15	PM,IS,SA
Pruebas de respaldo/restauración "local" via red local	1 día	Mie 11/4/15	Jue 11/5/15	PM,IS,SA
Pruebas de generación de informes avanzados via DPA	1 día	Jue 11/5/15	Vie 11/6/15	PM,IS,SA
Actualización de los manuales, diseño e informes de acuerdo al resultado de las pruebas	1 Sem	Vie 11/6/15	Vie 11/13/15	SA
Fin pruebas piloto de backup	0 días	Vie 11/13/15	Vie 11/13/15	
Pruebas piloto de securización	**3 días**	**Vie 11/13/15**	**Mie 11/18/15**	

Diseño de plan de pruebas de securización del sistema y conformidad a la regulación	2 días	Vie 11/13/15	Mar 11/17/15	SA
Ejecución del plan de pruebas	1 día	Mar 11/17/15	Mie 11/18/15	SA,IS
Fin pruebas piloto de securización	0 días	Mie 11/18/15	Mie 11/18/15	
FASE III - Puesta en producción de la solución	**9 días**	**Mie 11/25/15**	**Mar 12/8/15**	
Integracion final para producción del sistema con Lunitorización fabricante y respaldo de la plataforma/configuración	2 días	Mie 11/25/15	Vie 11/27/15	SA,IS
Configuración final de la plataforma y ajustes AVAMAR+DPA	1 día	Vie 11/27/15	Lun 11/30/15	IS
Integración del listado inicial de usuarios de respaldo remoto	1 día	Lun 11/30/15	Mar 12/1/15	IS
Realización de copia de respaldo del primer grupo de usuarios de respaldo remoto	1 Sem	Mar 12/1/15	Mar 12/8/15	IS
Conformidad del cliente a la plataforma	0 días	Mar 12/8/15	Mar 12/8/15	
FASE IV - Documentación y cierre	**3.5 días**	**Vie 12/11/15**	**Mie 12/16/15**	
Actualización de la documentación y procedimientos	3 días	Vie 12/11/15	Mie 12/16/15	SA
Entrega de la documentación y cierre formal de proyecto	4 hrs	Mie 12/16/15	Mie 12/16/15	SA,PM
Fin de proyecto	0 días	Mie 12/16/15	Mie 12/16/15	

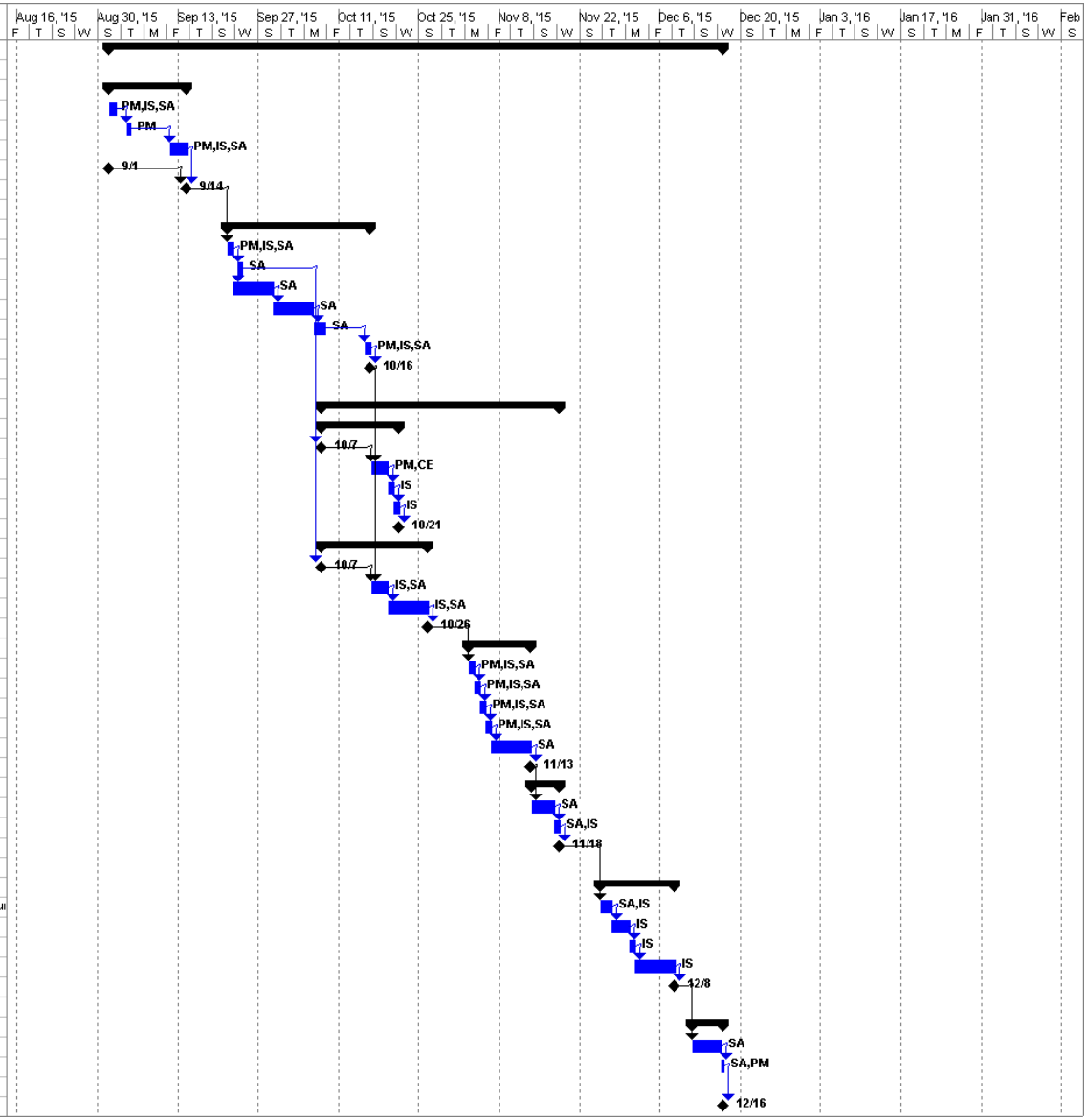
Tabla 7.Fases y Subfases del Proyecto.

Los recursos asignables son los siguientes:

- SA (*Solutions Architect)* – Arquitecto de de Sistemas.
- IS (*Implementation Specialist)* – Implantador de Sistemas.
- PM (*Project Manager)* – Jefe de Proyecto.
- CE (*Customer Engineer)* – Ingeniero de Soporte.

En la siguiente página se presentará el Diagrama de Gant del proyecto, donde se puede ver en detalle la línea temporal del mismo así como las relaciones entre tareas.

ID	Task Name
1	**AVAMAR + DPE (informes avanzados)**
2	
3	**FASE 0 - Arranque y Organización**
4	Reunión de arranque interno de proyecto
5	Creación del equipo de trabajo
6	Reunión de arranque externo de proyecto
7	Entrega del nuevo HW y licencias SW
8	Fin fase 0
9	
10	**FASE I - Diseño de la Solución**
11	Reunión de arranque técnico de diseño con cliente
12	Entrega de documento pormenorizado de requisitos de instalación
13	Elaboración del diseño y entrega del mismo
14	Elaboración de los manuales de administración y operación de la plataforma
15	Elaboración de los manuales de usuario
16	Revisión del diseño y manuales con cliente, correcciones y aceptación
17	Fin diseño global
18	
19	**FASE II - Puesta en marcha de la solución**
20	**Instalación de plataforma AVAMAR**
21	Fin de preparación de prerrequisitos de instalación HW
22	Ubicación física del nuevo HW, conexión eléctrica y LAN de los equipos
23	Configuración inicial, instalación/actualización de versiones FW
24	Integración de la solución con la monitorización y pruebas básicas de entorno
25	Fin instalación plataforma AVAMAR
26	**Puesta en marcha plataforma DPE**
27	Fin de preparación de prerrequisitos de instalación SW
28	Instalación del SW, configuración inicial
29	Preparación de los informes avanzados de acuerdo a la documentación de diseño y acuerdos con cliente
30	Fin instalación plataforma DPE
31	**Pruebas piloto de backup**
32	Pruebas de respaldo/restauración "remoto" via Internet
33	Pruebas de respaldo/restauración "local" via VPN
34	Pruebas de respaldo/restauración "local" via red local
35	Pruebas de generación de informes avanzados via DPA
36	Actualización de los manuales, diseño e informes de acuerdo al resultado de las pruebas
37	Fin pruebas piloto de backup
38	**Pruebas piloto de securización**
39	Diseño de plan de pruebas de securización del sistema y conformidad a la regulación
40	Ejecución del plan de pruebas
41	Fin pruebas piloto de securización
42	
43	**FASE III - Puesta en producción de la solución**
44	Integracion final para producción del sistema con monitorización fabricante y respaldo de la plataforma/configu
45	Configuración final de la plataforma y ajustes AVAMAR+DPA
46	Integración del listado inicial de usuarios de respaldo remoto
47	Realización de copia de respaldo del primer grupo de usuarios de respaldo remoto
48	Conformidad del cliente a la plataforma
49	
50	**FASE IV - Documentación y cierre**
51	Actualización de la documentación y procedimientos
52	Entrega de la documentación y cierre formal de proyecto
53	
54	Fin de proyecto



7.2 Desglose de gastos y presupuesto final

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor: Óscar Rivas Medina

2.- Departamento: Departamento de Informática

3.- Descripción del Proyecto:Implantación de Plataforma de Respaldo en la Nube

- Titulo	**Plataforma de Respaldo en la Nube**
- Duración (meses)	**2,5**
Tasa de costes Indirectos:	**20%**

4.- Presupuesto total del Proyecto (valores en Euros):

329,012.30 Euros

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F. (no rellenar - solo a titulo informativo)	Categoría	Dedicación (hombres mes)	Coste hombre mes	Coste (Euro)
Jefe de Proyecto		Ingeniero Senior	0.61	19,687.50	12,000.00
Arquitecto		Ingeniero Senior	2.44	16,406.25	40,000.00
Implantador		Ingeniero	1.58	9,843.75	15,600.00
Ingeniero de soporte		Ingeniero	0.06	9,843.75	600.00
					0.00
		Hombres mes	**4.69**	**Total**	68,200.00

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [a)]
AVAMAR	161,278.06	100	60	60	161,278.06
DPA (licencia por 5 años)	16,067.66	100	60	60	16,067.66
Coste equipos virtuales	1,310.83	100	60	60	1,310.83
		100		60	0.00
					0.00
				Total	178,656.55

[a)] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} x C x D$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado

B = periodo de depreciación (60 meses)

C = coste del equipo (sin IVA)

D = % del uso que se dedica al proyecto (habitualmente 100%)

SUBCONTRATACIÓN DE TAREAS

Descripción	Empresa	Coste imputable
n/a	n/a	0.00
	Total	0.00

OTROS COSTES DIRECTOS DEL PROYECTO

Descripción	Empresa	Costes imputable
Cableado estructurado	Cableados avanzados, SL	13,483.25
Alquiler de equipos PC portátil	Lenovo	9,000.00
Fungibles, viajes, dietas	Varios	4,837.12
	Total	27,320.37

6.- Resumen de costes

Presupuesto Costes Totales	**Presupuesto Costes Totales**
Personal	68,200
Amortización	178,657
Subcontratación de tareas	0
Costes de funcionamiento	27,320
Costes Indirectos	54,835
Total	329,012

Leganés a 9 de Julio de 2015

Fdo. Óscar Rivas Medina

Anexo I. Lista de comprobación para Proveedores de Servicios en la Nube.

Los entorno multicliente son una rareza en entornos dedicados, pero son excepcionalmente comúnes en plataformas en la nube. Esta diferencia es capital a la hora de establecer una valoración y análisis de riesgos, asi como las consideraciones legales y de privacidad que conlleva el servicio.

En este anexo se presenta una Lista de comprobaciones, la cual está pensada para ayudar al potencial cliente de Infraestructuras en la Nube tanto a tener en cuenta factores clave y expectativas que debe cumplir cualquier potencial Proveedor, asi como una manera objetiva de comparar entre varias ofertas.

Se espera del usuario de la Lista de comprobaciones que la envíe a los potenciales Proveedores de Servicio, y que una vez rellena, compruebe las respuestas, eligiendo el que fuese más apropiado para su caso concreto. Obviamente, cuantas más respuestas afirmativas se obtengan, mayor nivel de seguridad alcanzará el Proveedor.

En esta lista de comprobaciones se han obviado aspectos que tengan que ver con el precio de los servicios, los cuales pueden ser relevantes a nivel empresarial, pero no a efectos de este Proyecto de Final de Carrera.

Área	Asunto	Aspectos Específicos	Respuesta
Seguridad y Privacidad	Protección de Datos	Segregación de Datos	
		¿Cómo se separan mis datos de los de otros clientes?	
		Datos Almacenados	
		¿Dónde se guardan mis datos?	
		¿Qué nivel de cifrado se ofrece en mis datos almacenados?	
		¿Qué tipo de procedimientos de control y autenticación están implantados?	
		Datos en Tránsito	
		¿Cómo llegan los datos de mis instalaciones al Proveedor de Servicios?	
		¿Cómo se transmiten los datos en general?	
		¿Qué medidas se toman para evitar filtrados de información?	
		¿Puedo mantener una copia local de mis datos?	
		¿Alguna tercera parte puede acceder a mis datos? En caso afirmativo, ¿Quién? ¿Cómo?	
		¿Se puede asegurar el borrado de mi información si decido finalizar el servicio?	
	Gestión de Vulnerabilidades	Listado de evidencias del programa de gestión de vulnerabilidades.	
		¿Cada cuánto se buscan vulnerabilidades y errores en los sistemas?	
		¿Se pueden solicitar análisis de vulnerabilidad en la red del Proveedor de Servicio? ¿cómo?	
		¿Cuál es el proceso para solventar vulnerabilidades?	
	Gestión de Identidad	¿Puedo integrar mi servicio con mi propio sistema de autenticación? *Conviene asegurarse que esto no crea un riesgo de seguridad para mi propia infraestructura.*	
		En caso de no poder usar mi propio sistema de autenticación	
		¿Cómo se gestiona la seguridad de credenciales de acceso?	
		¿Cuál es el proceso de creación y borrado de usuarios?	
		¿Se soporta SSO (*Single Sign On*)? En caso afirmativo, ¿qué estandares?	
		¿Se soporta identidad federada? En caso afirmativo, ¿qué estandares?	
	Securidad Física	¿Existe acceso físco restringido o monitorizado 24x7 a las instalaciones?	
		¿Quién es el responsable de la seguridad de mis datos?	
		Si mi infraestructura fuese dedicada, ¿se puede asegurar que esté aislada del resto?	
		¿Existen medidas biométricas o similares para controlar los accesos?	
		¿Existe un procedimiento de acceso a las instalaciones físicas del proveedor?	
		Fecha y resultado de la última auditoría de seguridad realizada por un tercero.	
		Todos los empleados y personal de terceras partes deben portar y mostrar la identificación.	
		Todas las áreas perimetrales están monitorizadas por cámaras 24x7	

	Disponibilidad	¿Qué porcentaje de disponibilidad se garantiza?	
		¿Qué medidas se aplican para garantizar la disponibilidad ante ataques?	
		¿Se usan múltiples proveedores de servicios de internet?	
		¿Existen medidas contra ataques de denegación de servicio?	
		Informe con datos históricos de disponibilidad	
		Agenda de mantenimientos programados.	
		Datos acerca de la respuesta de los sistemas ante picos de carga	
	Seguridad de Aplicaciones	¿A qué tipo de pruebas y procedimientos de aceptacion se somete a las aplicaciones externas?	
		¿Qué medidas de seguridad se usan en el entorno de producción (cortafuegos a nivel de aplicación, auditoría de bases de datos, etc …)	
	Respuesta a Incidentes	¿Cuál es el procedimiento que se sigue ante fugas de datos?	
		¿Cuál es el tiempo medio de notificación de la incidencia?	
		¿En qué formato son las notificaciones, y que información contienen?	
	Privacidad	Garantías de que los datos críticos están correctamente enmascarados y que únicamente las personas autorizadas tienen acceso a los mismos.	
		¿Cómo se protegen los datos de usuarios de acceso y credenciales?	
		¿Qué datos se recogen acerca de un cliente? ¿Cómo se guardan? ¿Quién tiene acceso a los mismos?	
		¿Bajo qué condiciones terceros tienen acceso a mis datos? (Incluyendo agencias gubernamentales?	
		¿Se puede garantizar que el acceso por terceras partes a mis registros de actividad, no va a revelar información sensible acerca de mi actividad?	
Conformidad	Continuidad de Negocio y Recuperación ante Desastres	¿Se tienen procedimientos de Continuidad de Negocio o Recuperación tras Desastres?	
		Asegurarse que estos procedimientos son, al menos, tan robustos como los propios.	
		¿Se pueden auditar estos procedimientos?	
		¿Dónde están localizados los Centros de Proceso de Datos de respaldo?	
		¿Qué nivel de servicio pueden garantizar los centros de respaldo?	
	Registros y Auditoría	¿Se pueden realizar Análisis Forenses en la infraestructura?	
		¿Se pueden mantener los registros tanto tiempo como deseemos?	
		¿Se puede tener almacenamiento dedicado para los registros?	
		¿Existe algún método para garantizar que no se puede alterar maliciosamente los registros?	
	Requerimientos específicos	¿Se cumple con las regulaciones locales en los Centros de Proceso de Datos?	
		¿Las regulaciones locales entran en conflicto con las nuestras?	
		¿Se cumple con la ISO-27001?	

Otros	Responsabilidad	Comprobar la localización geográfica de mis datos en todo momento.	
		¿Puede el proveedor forzarnos a cumplir determinadas condiciones legales? ¿Cuáles?	
		¿Se puede comprobar la conformidad con la LOPD?	
		¿Cuáles son los acuerdos de restitución en caso de brecha de seguridad o incumplimiento de las SLA?	
		Bajo que condiciones?	
	Propiedad Intelectual	Es necesario que, de manera contractual, se mantenga la propiedad de los datos en nuestra parte.	
	Soporte de fin de Servicio	¿Qué ocurre en el periodo de finalización del servicio?	
		¿Se devolverán los datos? ¿En qué formato?	
		¿Cuánto tardaré en recuperar mis datos?	
		¿Se eliminaran mis datos totalmente de la infraestructura? ¿En cuánto tiempo?	
		¿Habría que pagar alguna tasa adicional al finalizar el servicio?	
	Bloqueo de Proveedor	¿Se puede garantizar la migración de datos y/o aplicaciones a otros proveedores o infraestructura propia de la organización?	

La lista de comprobaciones anterior está basada en recomendaciones generales realizadas por autoridades de seguridad en Computación en la Nube (En concreto Forrester Research, Symantec y eSentire Inc.), y también basándonos en el marco legal aplicable en España, el cual hemos tratado en puntos anteriores.

Referencias

1 P. Mell, T. Grance – *The NIST Definition of Cloud Computing.* Septiembre 2011. Disponible [Internet]: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [Marzo de 2015].

2 Information Systems Audit and Control Association – *Essential characteristics of Cloud Computing*. Disponible [Internet]: http://www.isaca.org/groups/professional-english/cloud-computing/groupdocuments/essential%20characteristics%20of%20cloud%20computing.pdf [Febrero de 2015].

3 P. Mell, T. Grance – *The NIST Definition of Cloud Computing.* Septiembre 2011. Disponible [Internet]: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [Marzo de 2015].

4 Gartner Technology Research – *Gartner Executive Programs Worldwide Survey of More Than 2,000 CIOs Identifies Cloud Computing as Top Technology Priority for CIOs in 2011*. Enero 2011 Disponible [Internet]: http://www.gartner.com/it/page.jsp?id=1526414 [Mayo de 2015].

5 The OpenGroup – *Convergent Technologies Survey*. Septiembre de 2013. Disponible [Internet]: https://www2.opengroup.org/ogsys/catalog/R130 [Abril de 2015].

6 T. J. Bittman - Gartner Technology Research - Steps to Operationalize Private Cloud Computing. Febrero de 2012. Disponible [Internet] https://www.gartner.com/doc/1937017/steps-operationalize-private-cloud-computing [Junio de 2015].

7 Cloud Standards Customer Council - *Migrating Applications to Public Cloud Services: Roadmap for Success*. Diciembre de 2013. Disponible [Internet] http://www.cloud-council.org/Migrating-Apps-to-the-Cloud-Final.pdf [Junio de 2015].

8 Claus Pahl, Huanhuan Xiong, Ray Walshe - IC4, Dublin City University - A Comparison of On-premise to Cloud Migration Approaches. Disponible [Internet] http://doras.dcu.ie/18475/1/migration.pdf [Junio de 2015].

9 Benedikt Martens, Frank Teuteberg - University of Osnabrueck - *Risk and Compliance Management for Cloud Computing Services: Designing a Reference Model* [Mayo

de 2011]. Disponible [Internet] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.231.6718&rep=rep1&type=pdf [Mayo de 2015].

10 The University of Sydney – *The TJX Data loss and security breach case* [Octubre 2007]. Disponible [Internet] http://sydney.edu.au/engineering/it/~info5990/Supplements/Week07_Malware&Security/Supp07-4TJXCaseDetails.pdf [Mayo de 2015].

11 Rachael King – Blooomberg Bussiness - *Lessons from the Data Breach at Heartland* [Julio de 2009]. Disponible [Internet] http://www.bloomberg.com/bw/stories/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice [Abril de 2015].

12 Cloud Security Alliance – *The Notorious Nine Cloud Computing Top Threats in 2013* [Febrero de 2013]. Disponible [Internet] https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf [Mayo de 2015].

13 European Union Agency for Network and Information Security - *ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats* [Diciembre de 2014]. Disponible [Internet] https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf [Junio de 2015].

15 Ernest & Young – *Governing the Cloud*. Disponible [Internet] http://www.ey.com/GL/en/Services/Advisory/governing-the-cloud [Mayo de 2015].

16 J. Oriol Fito, Jordi Guitart – Universidad de Cataluña - *Introducing Risk Management into Cloud Computing* [2010]. Disponible [Internet] https://upcommons.upc.edu/e-prints/bitstream/2117/15944/1/Fito.pdf [Mayo de 2015].

17 Portal de Administración Electrónica – *Leyes y normas reguladoras de ámbito estatal* [Mayo de 2015]. Disponible [Internet] http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_LegNacional/pae_NORMATIVA_ESTATAL_Leyes.html#.VXVgt5Pl_AW [Junio de 2015].

19 A. Cavoukian - *Privacy by Design: Los 7 Principios Fundamentales* [Febrero de 2011]. Disponible [Internet] https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf [Mayo de 2015].

20 H.Rifà, J. Serra, J. Rivas - UOC 2009 – *Análisis Forense de sistemas informáticos* [Septiembre de 2009]. Disponible [Internet] http://jlrivas.webs.uvigo.es/downloads/publicaciones/Analisis%20forense%20de%20sistemas%20informaticos.pdf [Marzo de 2015].

21 Agencia Española de Protección de Datos – *Guía para clientes que contraten servicios de Cloud Computing* [2013]. Disponible [Intenet]

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf [Junjo de 2015].

23 U. Fisher - Information Systems Audit and Control Association - *A IT Value Delivery, Risk IT, CobiT, Val IT und ITIL* [Abril de 2010]. Disponible [Internet] http://www.isaca.org/Groups/Professional-English/it-value-delivery/GroupDocuments/swissforum_ValueDelivery_Fischer.pdf [Junio de 2015].

24 J. Huang, D. Nicol – Journal of Cloud Computing - Trust mechanisms for cloud computing [Abril de 2013]. Disponible [Internet] http://www.journalofcloudcomputing.com/content/2/1/9# [Junio de 2015].

25 A. Haeberlen – Max Plank Institute for Software Systems - A Case for the Accountable Cloud. Disponible [Internet] http://zoo.cs.yale.edu/classes/cs426/2013/bib/haeberlen09acase.pdf [Junio 2015].

Bibliografía

EMC Computer Systems. (Septiembre de 2012). *Virtualized Datacenter and Cloud Infrastructure Planning and Design*.

EMC Computer Systems. (2013). *EMC Avamar Security Guide.*

EMC Computer Systems. (2015). *EMC Avamar Administration Guide*. Obtenido de http://support.emc.com.