SEGURIDAD DE CABLEADO Y DATACENTER

Unidad 2

Seguridad de Almacenamiento en el Datacenter

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar: Eder Morán Heredia

Diseñadora instruccional: Luisa García Ospina

Editora instruccional: Trinidad Marshall

VALIDACIÓN

Experto disciplinar: Gabriel Urra Varas

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Welearn

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Configurar redes definidas por software, considerando respaldo de datos en datacenter y computación de nube.

Fuente: https://image.shutterstock.com/image-photo/male-specialist-holds-laptop-discusses-600w-1062915392.jpg

Introducción

¿Qué es una copia de Seguridad?

En las últimas décadas, la computación en la nube y los SaaS (Software as a Service) han impulsado el desarrollo computacional y la transformación digital. Este nuevo tipo de tecnologías permiten el mejoramiento de la gestión, administración y monitoreo de los datos por medio de una nube que las guarda. Así, la Nube computacional se transformó en una de las herramientas facilitadoras de la nueva era digital. Además, los SaaS han sido innovadores a la hora de generar recursos más eficientes para la administración de la gestión de datos.

Uno de los grandes desafíos de las empresas es romper los mitos relacionados a los servicios en la nube y, sobre todo, como operan los sistemas de seguridad en la infraestructura de los iCloud. Algunos ejemplos de la operatividad de la ciberseguridad en la nube se pueden encontrar en servicios como Amazon Web Service (AWS) y Google Cloud Platform (GCP). En estas plataformas se encuentra la infraestructura tecnológica entre otros proveedores de servicios Cloud como Microsoft Azure, los cuales están dando la pauta de ofrecer un servicio con estándares de seguridad de clase mundial. Por ello, las empresas están obligadas a soportarse tecnológicamente en este tipo de plataforma ya que son las más seguras a nivel planetario. Asimismo, es importante destacar que los pasos que debemos seguir para proteger la información es un procedimiento basado en los estándares establecidos bajo un determinado ordenamiento.

1. -Seguridad en redes basadas en computación de nube

La prestación de servicios en la nube ha cambiado la forma de ver como consumimos las tecnologías y adoptamos sistemas de todo tipo. Atrás quedó el modelo de distribución de licencias para dar paso a un enfoque mucho más orientado a los servicios. Actualmente, se han modificado las operaciones tecnológicas en todo tipo de organización sin importar el tamaño, la industria o la geografía, gracias a este tipo de servicios tecnológicos.

Este fenómeno trae grandes desafíos en materias de seguridad, tanto el Cloud Computing como en la ciberseguridad, y se han convertido en los puntos que encabezan las listas de prioridades de las empresas con un alto componente tecnológico.

¿Cuáles son los rumbos que hacen las empresas en materia de Seguridad?

Los principales proveedores de servicios en la nube como Amazon Web Service o Google Cloud realizan controles de seguridad en la nube verificando en forma independiente las políticas de privacidad y cumplir con el establecimiento de informes a disposición de las empresas. Por lo tanto, el rumbo que han tomado las empresas con respecto a la Ciberseguridad es la aplicación de estos servicios para resguardar eficientemente los datos.

Tendencias de Ciberseguridad.

Ante los grandes volúmenes de datos y la creciente información que deben manejar los especialistas y las actualizaciones que han surgido, se requerirán nuevos tipos de habilidades en ciencias de datos y análisis, haciendo de la inteligencia de seguridad artificial algo imprescindible. Por ello, las empresas deben considerar fundamentalmente la inversión en estrategias de detección y respuesta, y parte del presupuesto debe estar enfocado en prevención del riesgo y los ataques.

Sin embargo, no todo se puede prevenir, pero, sí es posible saber cómo responder, y es el terreno de la detección, respuesta y solución donde debe hacer foco la ciberseguridad moderna. La adopción del Cloud computing es el más usado por todas las empresas del mundo, y, en ella se han sumergido para el mejoramiento de la seguridad de datos. Ante esta situación, la necesidad de protocolos y normativas de seguridad a nivel internacional ha sido urgente y efectivo. A continuación, trataremos algunas de las normas internacionales establecidos con el objetivo de tomar medidas de seguridad sobre información en la nube.

Normas ISO de Ciberseguridad.

Cuando trabajamos con información en la nube, las empresas que prestan el servicio deben asegurar la integridad de los datos de los clientes o del usuario final dentro de las normas ISO 27017, 27001, y 27018. Éstas apuntan a fortalecer la ciberseguridad en servicios Cloud. A continuación, te contamos todo lo que necesitas saber al respecto.

Para elegir un proveedor de servicios en la nube se debe revisar si esto cuenta con un certificado ISO dentro de sus políticas de seguridad. Dicha certificación deberá establecer y garantizar los altos estándares en la seguridad de la información. El tipo de empresas que están aseguradas con este tipo de certificaciones son aquellas que prestan servicios DBaaS (Data Base as a Service) y SaaS (Software as a Service).

En estas normativas se deben constituir los principales estándares para resguardar la ciberseguridad y garantizar la integridad de la información alojada en la nube. Estos servicios son ofrecidos por empresas como Amazon Web Services (AWS), Google Cloud o Microsoft Azure.

ISO 27001:

La norma ISO 27001 es un estándar generado por la ISO (Organización Internacional de Normalización), el cual describe la manera correcta de gestionar la seguridad de la información al interior de una organización. Se trata de la principal norma a nivel global para el manejo de la información el cual es usado por la mayoría de las empresas usuarias de plataformas de seguridad de la nube. Su principal eje es el sistema de Gestión de Seguridad de la Información (SGSI), el cual debe realizar a través de un proceso sistemático, documentado y conocido por toda la organización.

La norma establece que las organizaciones conozcan los riesgos asociados al manejo de información, asumiéndolos minimizándolos y gestionándolos por medio de un proceso documentado, sistemático, estructurado, eficiente, repetible y

adaptable a los eventuales cambios que pudieran presentar los riesgos. El entorno y la tecnología para obtener la certificación la organización deben cumplir con ciertos pasos:

- Etapa Previa: Aquí, las empresas deben implementar 14 pasos básicos para iniciar la certificación. Entre los principales está el uso de una metodología de gestión de proyecto, contar con el apoyo de la dirección en el proceso de implementación, definir el alcance del sistema de seguridad, determinar una política e evaluación de riesgos, implementación de controles y medidas correctivas.

- Auditoria de Revisión: Tanto Externo como Interno, el personal adecuado para ello revisa si cumplen con los lineamientos para el proceso de certificación.

- Auditoria Principal: Aplicado por un grupo de auditores quienes verificarán las medidas establecidas que cumplan los objetivos y, de estar todo en orden, la empresa puede ser certificada.

- Revisiones Periódicas: Luego de obtener las certificaciones, el organismo encargado deber monitorear dicha empresa durante 3 años para garantizar que cumpla con los esfuerzos de protección de datos.

ISO 27017:

La norma ISO 27017 es un estándar de seguridad que proporciona controles para los usuarios finales, los clientes y a los proveedores de servicios en la nube. Su importancia radica en la precisión con la que establece las relaciones entre el usuario y proveedores de servicios en la nube, determinando las exigencias al cliente y el rol del proveedor de establecer la información otorgada.

El cumplimiento de esta norma establece la ciberseguridad y la gestión de servicio referente a la arquitectura, medidas de seguridad, funcionalidades disponibles, tecnología de cifrado y localización geográfica de datos. Además, establece 37 controles en la nube los cuales se basan en la ISO 27002, junto a 7 adicionales que permiten fortalecer la seguridad de los servicios Cloud.

ISO 27018:

Finalmente, la norma ISO 27018 constituye un compendio de buenas prácticas referentes a controles de protección de datos para servicios Cloud, y se enfoca específicamente en los proveedores. El objetivo es delimitar las normas y procedimientos dentro de los controles de los proveedores en su calidad de procesadores de datos. Para ello, deben aplicar la garantía en el cumplimiento de la norma en cuanto al manejo de los datos personales.

Proveedores de Servicios Cloud con las normas ISO.

Entre los proveedores más conocidos está Amazon Web Services (AWS), que visualiza el cumplimiento de todas las normativas anteriores. Además, cumple con leyes y regulaciones específicas de determinados países. Asimismo, Google Cloud es otro proveedor que pone a disposición de los usuarios el listado de normativas, certificaciones y regulaciones con que cumple para garantizar la ciberseguridad de los datos de sus clientes.

Por otro lado, en el caso de Microsoft Azure tiene una vasta experiencia en la venta de software empresarial para la construcción de la infraestructura de una nube segura. La seguridad establecida por Microsoft Azure es confiable debido a que cuenta con todas las certificaciones ISO pertinentes al resguardo de datos.

Por ello, contar con estas certificaciones le ha permitido a AWS, a Google Cloudy, y a Microsoft Azure posicionarse como los mejores proveedores de servicios en la nube, y, tanto el modelo DBaaS como el SaaS, se han vuelto más seguros, confiables, transparentes y efectivos.

Ataques DDOS en la Nube.

Conocido como el peor ataque de un administrador de sistemas, los ataques DDoS (Distributed Denial of Service, Denegación de Servicio Distribuido) pueden causar grandes pérdidas en redes corporativas y costar a las empresas importantes sumas de dinero en caso de no estar preparados. Mientras que los más afectados son quienes cuentan con un servidor local propio, los más perjudicado son mayormente aquellos que usan sistemas de cómputo en la nube. Por lo tanto, hay que considerar

que no están exentos de amenazas, para ello estableceremos algunas prácticas para prevenir y mitigar este tipo de ataques en configuraciones de cloud computing.

Un ataque DDoS (Distributed Denial of Service) es el proceso de agotar los recursos disponibles para una red, aplicación o servicio con tal que el usuario final no pueda acceder al sistema vulnerado. El aumento del "Hacktivismo" ha provocado un aumento en el uso de los ataques DDoS, ligado a la innovación en las áreas de herramientas, objetivos y técnicas usadas para su ejecución. Actualmente, los Hackers usan una combinación de ataques de gran volumen, junto con infiltraciones más sutiles y difíciles de detección. Además, apuntan hacia las aplicaciones así como a la infraestructura de seguridad de red existente, como firewalls e IPS. Para la construcción de un sistema de protección contra intrusiones para evitar este tipo de ataques debemos desarrollar los siguientes pasos:

- Desarrollando soluciones Escalables: Contar con una infraestructura escalable es fundamental para un sistema bien establecido. Además de tener una técnica de gran efectividad a la hora de evitar ataques DDoS para cumplir con los volúmenes de trafico adicionales, ya sean válidos o de un ataque DDoS.

- Minimizando el área de superficie de ataque: En este caso es clave desacoplar las partes de su infraestructura de red al ejecutar los sitios web públicos, separa la aplicación de la base de datos, los medios y su contenido estático también. Las aplicaciones desacopladas limitan el acceso a internet a los componentes críticos del sistema, protegiéndose de un ataque. También es necesario establecer procedimientos para la mitigación de un ataque.

- Aislando el tráfico interno de la Red exterior: Implementando instancias sin IP públicas, a menos que sea necesario. Por ejemplo, configurando una puerta de enlace NAT o un bastón SSH para limitar el número de instancias que están expuesta en internet.

- Equilibrando la carga con la ayuda de Proxys: AWS y Google Cloud poseen herramientas de balance de carga HTTP(s) o balance de carga SSL proxy. A la infraestructura de sus servidores Cloud es capaz de mitigar y absorber muchos ataques de Capa 4, a los de inundación SYN, inundación de fragmento de IP, etc. Al contar con un balanceador de carga HTTP(s) logra dispersar cualquier posible ataque a través de las instancias de sus servidores alrededor del globo.

Protección de Datos.

En el presente proceso de transformación digital, cada vez más empresas trasladan sus datos a la nube. En este aspecto, la ciberseguridad es uno de los temas más importantes, como por ejemplo en las cargas de trabajo en la nube, evidencia la importancia que los servicios de Cloud tiene para la evolución de las organizaciones en un mercado más digitalizado y competitivo.

Las empresas que ofrecen los servicios de DBaaS deben implementar estrictas medidas de seguridad para no comprometer la información de los usuarios. En el caso de Google cloud, la compañía cuenta con más de 750 expertos encargados de mantener los sistemas de defensa y crear la infraestructura. En la implementación de

las políticas de seguridad es importante destacar que la seguridad de almacenamiento en la nube dependerá de dos factores: Cliente y Proveedor.

Al Proveedor le compete la seguridad de la nube, mientras que el Cliente protege los componentes del sistema operativo alojamiento y las instalaciones físicas, por lo tanto, es un modelo de responsabilidad compartida. El Cliente debe vigilar las plataformas, sistemas, aplicaciones, y configurar redes, además de prestar especial atención a los permisos y la privacidad con la que los usuarios acceden a sus plataformas en la nube. Siendo así, es el Cliente quien controla la arquitectura de seguridad, la fuerza de sus contraseñas.

¿Dónde se almacenan los Datos en la Nube?

Para tranquilidad de los usuarios, los datos son almacenados y resguardados con estrictos controles de seguridad en los servidores de los centros de datos del proveedor. Por medio de una protección mayor a la que tendrían dentro del área de IT de una empresa, estos centros están ubicados en diversas localizaciones, y cada cliente determina la región y el servidor donde desea alojar sus datos.

¿Quién puede acceder al contenido?

Solo los clientes pueden manejar el formato, estructura y claves de cifrado de los datos, y son ellos los únicos que deciden a quienes facultan para acceder a determinada información.

Los principales proveedores de DBaaS son Google Cloud, Microsoft Azure y AWS ya que ofrecen ciberseguridad, privacidad, transparencia y cumplimiento de las normas

internacionales garantizado a través de auditorías y certificaciones para mantener una base de datos en la nube.

Características de los Servicios Cloud.

- Servicios bajo demanda: En los casos que se ofrece el servicio de la nube, los clientes tienen la opción de aprovisionarse de capacidades de cómputo tales como el aumento de los recursos de memoria, espacio en disco o core de aprovisionamiento de acuerdo a las necesidades que se lleguen a presentar.

- Pago por Capacidades: Los modelos de facturación están basados en los recursos usados, y esto es debido a que el cliente paga según las variaciones en las capacidades que use.

- Acceso en cualquier momento: Permite a los usuarios ingresar a los servicios contratados en Cloud desde cualquier parte del mundo, solo deberá contar con un dispositivo que tenga disponible un servicio de internet.

- Agilidad de Aprovisionamiento: Los usuarios del servicio pueden aprovisionar de manera rápida, y en algunos casos de manera autónoma, los recursos que lleguen a ser necesarios. De tal forma, los clientes tienen la capacidad de aprovisionarse con los recursos que se tengan disponible y la posibilidad de pagar en cualquier momento.

Beneficios para empresas en Cloud.

Las empresas con sus servicios en la nube tienen la necesidad de que los proveedores apliquen buenas prácticas, y estas deben ser las adecuadas para brindar la seguridad requerida. A razón de esto, se crea la necesidad de cumplir con los requisitos en materia de seguridad en las instalaciones, requisitos legales, limitaciones políticas y técnicas, para ello se debería contar con los siguientes pasos:

- Evaluación de Riesgos de Servicios en Cloud.
- Identificar las ofertas de los proveedores.
- Verificar la seguridad de los proveedores.
- Transferir cargas de la operación de seguridad a los proveedores.

- Recomendaciones Legales: Gran parte de los requisitos legales vinculados a la Cloud se solucionan en la evaluación de los riesgos asociados. En ellos, se comparan los beneficios o deficiencias de los distintos proveedores de servicios, y la forma más real es la revisión de los contratos de forma más detallada como las cláusulas que los contiene. Así se establecen derechos y obligaciones en el área de requisitos de seguridad intercambio de datos, control de cambios, controles de acceso.

- Principales Ventajas: Se establece la nube con referencia a las arquitecturas de la computación que pueden soportar, y esto se debe a la dimensión. Para la implementación de estrategias se obtienen una mejor protección, por ende, a bajos precios se pueden adquirir filtrado de navegación, gestión de

actualizaciones, aseguramiento de sistemas de virtualización, infraestructura distribuida, mejores respuestas a incidentes y gestión de amenazas.

- Creando diferencias con la seguridad: Es una prioridad para las empresas, sobre todo aquellas que prestan servicios en la nube. La mayoría de las empresas que deciden migrar servicios en la nube tiene en cuenta tres pilares de la seguridad: Confidencialidad, Integridad, y Disponibilidad, pero aún más importante la Resiliencia.

- Auditoria y gestión de evidencias: En los sistemas de computación, la principal infraestructura de una nube es un ambiente virtualizado. Estos sistemas pueden proporcionar imágenes forenses de las máquinas virtuales que pueden verse afectados, sin necesidad de desconexión a la red.

Riesgos para empresas en Cloud.

Los riesgos más importantes se presentan a continuación:

Perdida de gobierno: Al realizar la migración de los recursos en la nube, los usuarios ceden el control de diversos parámetros y dispositivos que influyen directamente en la gestión de la seguridad. Tanto el cliente como los proveedores, pueden llegar a pasar en los acuerdos de nivel de servicio o al contrato donde no se incluyen los servicios por parte de los proveedores creando fallas en las defensas.

Vinculación: Cuando tenemos infraestructura dedicada a proveedores en la nube o viceversa, las herramientas procedimientos, formatos y ampliación de estándares

que aseguran la migración de los servicios no sean necesariamente implementados. Esto genera cuando un cliente quiera emigrar sus servicios a otro proveedor sea más complejo que lo esperado.

Aislamiento: Al tener una infraestructura que permita la disrupción de recursos y asignarlo a diferentes clientes es una de las características para los proveedores en servicios en la nube permiten presentar fallas en los proceso que separan lo recursos como procesamiento además se presenta con dificultades para un atacante

Cumplimiento: La migración de los servicios en la nube puede afectar por el cumplimiento de requerimientos obligatorios o normas establecidos por los países de los clientes. Por algún motivo algún cumplimiento de los requerimientos o normas, los proveedores realizan auditorias de infraestructura, por lo tanto, adquirir servicios en la nube no implica adquirir diversos niveles de los requerimientos o normas.

Interfaz de Gestión: Los proveedores de servicios en la nube pueden en algún momento publicar a internet las interfaces de gestión de las plataformas que soporta la infraestructura donde se centraliza la administración de los recursos. Por lo tanto, es un riego que puede presentarse con el acceso remoto a las plataformas de gestión o vulnerabilidades que se presenten en los navegadores web.

Para ello, se deben realizar algunas prácticas que permiten la protección y la seguridad. En la actualidad muchos usuarios usan los servicios Cloud sin saber que lo realizan de esta forma y es desarrollado por la implementación y administración adecuada de los recursos con buenas prácticas tales como:

- Encriptación: No solo el envío de la información en la nube, sino el alcance debe llevar en un entorno tecnológico donde la información pasa por varios dispositivos antes de su destino fatal. En los sistemas Cloud, los proveedores recomiendan cifrar los canales de comunicaciones desde los clientes hasta los proveedores.

- Políticas de Almacenamiento: Este básicamente depende del tamaño de la información almacenada, y pueden existir variantes donde no se usen partes de esta información. Para ello, se deben establecer políticas donde se revise la información almacenada.

- Políticas basadas en roles: El establecimiento de roles y políticas de los usuarios es importante para segregar de manera correcta y establecer sus privilegios. Esto permite establecer quien hace qué, cuándo lo utiliza y el motivo principal del acceso.

- Software como servicio: Brindan a sus clientes una arquitectura multitarea, en algún momento que se llegue a presentar una falla de los servicios puede afectar a varios clientes. Por ello, se recomienda usar una arquitectura VPN (virtual prívate network), y la AWS (Amazon Web Service) ofrece este tipo de servicio en donde una instancia virtual se brinda el control completo.

- Cumplimiento: Las empresas que quieran contar con sus servicios en Cloud siempre están sujetos a regulaciones de los países donde se encuentran, por lo que, al escoger un proveedor, se debe verificar si las políticas de estos se ajustan a las solicitadas por los gobiernos.

2. -Planes de respaldo y recuperación de datos

Una empresa prospera cuando la información es disponible en el momento necesario, de lo contrario, causaría un impacto inmediato en la productividad, en la satisfacción de los clientes y en los beneficios. La disponibilidad de la información está directamente relacionada con la flexibilidad empresarial, y los desastres pueden destruir grandes volúmenes de datos y trabajo, y tener efectos devastadores en la viabilidad del negocio. Debido a esto, es importante aclarar los diferentes tipos de copias de seguridad a nivel general que existen y como deben llevarse a cabo en los procesos de respaldo de información.

Tipos de respaldo de información:

- Copia de seguridad Completa: Es el punto de partida para el resto de las copias de seguridad y contiene todos los datos de las carpetas y archivos que maneja el sistema. Por lo general, resultan y dan como resultado operaciones de restauración más rápidas y más simples. La limitante son los tiempos en los procesos de copiado, por lo que limitan el horario semanal o mensual, aunque el aumento de la velocidad y la capacidad de los medios hacen que sean posibles que los horarios de trabajo se detengan específicamente en los horarios nocturnos.

- Copia de Seguridad Incremental: Almacena todos los archivos modificados desde el último respaldo completo, diferencial o copia de seguridad incremental. La desventaja es que durante una operación de restauración

cada incremento se procesa, lo que resultaría en un proceso largo. Sin embargo, proporciona un método más rápido de copia de seguridad de datos, en el caso de la forma incremental solo los archivos modificados desde la última copia de seguridad. Además, se incluye en cada copia de seguridad el cual aumenta de una anterior, y el tiempo de copiado es menor en comparación a una copia de seguridad completa. El programa Backup4all es un programa que admite copias de seguridad incrementales y usa la información registrada. La ventaja de los tiempos de seguridad más bajos es que el tiempo de restauración tiene un precio. Al restaurar cada copia de seguridad incremental se necesita el respaldo completo más reciente, así como cada copia de seguridad.

- Copia de Seguridad Diferencial: Contiene todos los archivos que han cambiado desde la última copia de seguridad completa. La ventaja de una copia de seguridad diferencial es que disminuye el tiempo de restauración, en comparación con una copia de seguridad completa o copia de seguridad incremental. Sin embargo, si se realiza varias veces el tamaño de la copia de seguridad diferencial podría ser más grande que la completa inicial.

Algunas Soluciones Externas.

Varias empresas, cuyo objetivo es el desarrollo eficiente de la realización de BackUp, se han visto en la necesidad de proteger la continuidad de los negocios y

contrarrestar las preocupaciones con respecto a la perdida de información. Para ello, se soportarán por varias herramientas digitales como las siguientes:

- Bacula, Open Source basado en la red: Es un conjunto de programas que le permite al administrador del sistema gestionar copias de seguridad y verificación de los datos de la computadora. Esto a través de máquinas de diferentes tipos y pueden ejecutar por completo en un solo ordenador y hacer copias de seguridad de varios tipos de medios basado en Cliente/servidor de red fácil de usar y eficaz.

- Symantec: Es un producto integrado que protege entornos físicos y virtuales, simplifica las copias de seguridad y la recuperación después de un desastre. También, ofrece capacidades inigualables de recuperación basado en la tecnología V-Ray de Symantec, y es posible restaurar servidores enteros aplicaciones críticas de Microsoft y entonos virtuales VMware.

- Amazon S3-Backup´s online: Ofrece un entorno altamente resistente, escalable y seguro para la copia de seguridad y el archivado de sus datos más importantes. Se hace uso del control de versiones Amazon S3 para proteger aún mejor sus datos almacenados, si cuenta con un conjunto de datos de un tamaño significativo es posible establecer el traslado de grandes cantidades de datos hacia y desde el AWS usando dispositivos de almacenamiento físicos.

Metodologías propuestas: Para hacer uso de las metodologías propuestas se debe tener en cuenta el ciclo de vida del proceso el cual consiste en la gestión de procesos, desde la creación hasta la finalización. Estos cinco elementos básicos son:

- Estrategias del proceso: Determina los tipos de proceso que deben ser realizados.
- Diseño del proceso: Identifica los requisitos del proceso y elabora nuevos procesos.
- Transición del Proceso: genera e implementa procesos nuevos o modificados.
- Operación del Proceso: Lleva a cabo las tareas operativas.
- Mejora continua del proceso: Aprende de los éxitos y fracaso del pasado y mejora constantemente la eficiencia de los procesos.

Para un buen manejo de la información recopilada también existen una serie de recomendaciones de los estándares que se manejan y dan aporte en cuanto a la forma como los proceso de guardar la información se ciñen a dichos estándares.

Estándar ISO/EC 27002: En los estándares de la información se encuentra la ISO/IEC (International Organization for Standarization/ International Electrotechnical Commision) en la serie 27000 se encuentra la norma 27002 que muestra una guía de buenas prácticas y lineamientos para el correcto manejo de la información según el apartado 10.5 se menciona algunas recomendaciones acerca de las copias de seguridad:

Apartado 10.5: Respaldo o Back-Up.

Objetivo: Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información, se deben establecer los procedimientos de rutina para implementar la política de respaldo y la estrategia (ver también 14.1) para tomas de copias de seguridad.

Control: Se deben hacer copias de respaldo de la información y software y se deben probar regularmente en concordancia con la política de copias de respaldo acordada.

Lineamientos de Implementación: Se deben proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y software se puedan recuperar después de un desastre o falla de medios se deben considerar varios ítems. Se deben establecer el nivel necesario de respaldo de información. Se deben producir registros exactos y completos de las copias de respaldo y procedimientos documentados de restauración.

La extensión (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos deben reflejar los requerimientos comerciales de la organización, los requerimientos de seguridad y el grado crítico de la información. Las copias de respaldo se deben almacenar en un lugar apartado la distancia suficiente como para escapar de cualquier daño por un desastre.

A la información de respaldo se debe dar el nivel de protección física y ambiental apropiada consistente con los estándares aplicado en el local principal. Los medios de respaldo se deben probar regularmente para asegurar que se puedan confiar en

ello para usarlos cuando sea necesario en caso de emergencia. Los procedimientos de restauración se deben chequear y probar regularmente para asegurar que sean efectivos y que puedan ser completados dentro del tiempo asignado. En situaciones cuando la confidencialidad es de importancia, las copias de respaldo deben ser protegidas por medio de codificación.

3. -Creación de imágenes y copias de seguridad

¿Cuál es la diferencia entre "Hacer una copia de seguridad" y "Hacer una imagen del sistema"? ¿Guardan los mismos archivos y si es así, por qué el sitio web muestra ambos métodos?

La elección del tipo de copia de seguridad adecuado para un dispositivo depende del tipo de datos y de los riesgos a los que enfrenta tu dispositivo en la categoría de diversas circunstancias de perdida de datos. Si se establece entre la copia de seguridad y la imagen del sistema al menos se debe conocer los enfoques de los tipos de copias de seguridad.

En este caso, la copia de seguridad simple es aquella que cubre todos los archivos de la información del dispositivo o la copia de seguridad de una partición, sector o carpeta específicos, etc. Mientras que, como su nombre lo indica una copia de seguridad del sistema es creada para hacer un clon de un archivo del sistema (sistema operativo, actualizaciones del sistema. Controladores del sistema, archivos del sistema, aplicación, puntos de restauración del sistema, etc.).

¿Por qué es necesario crear una copia de seguridad del sistema?

Se crea una copia de seguridad del sistema/imagen del sistema después de la actualización o de nuevas aplicaciones, se crea cuando se ejecuta una instalación limpia para deshacerse de todos los virus y ataques de malware y hacer correcciones. La imagen del sistema actúa como un punto de restauración del sistema operativo que se usa más tarde para rehabilitar nuevamente el sistema operativo a la restauración de trabajos anteriores.

Una imagen del sistema es importante cuando se pretende sustituir el disco duro por uno nuevo, podría ser un disco duro defectuoso o un problema de almacenamiento. Lo que al final resulta en el remplazo de la unidad defectuosa, por lo tanto la creación de una imagen del sistema te proporciona herramientas que te ayudaran a migrar todos los datos del sistema en el nuevo disco duro y te ahorrara tiempo para omitir la reinstalación del sistema operativo y los elementos importantes asociados.

Mediante la creación de una imagen del sistema, puedes hacer frente a los errores relacionados con el sistema operativo o el disco duro.

Imagen del Sistema: Tiene que ver con el sistema operativo, su servicio se ocupa de crear una copia del sistema operativo. Se realiza para proteger el sistema operativo o de una caída del sistema, rehabilitar el dispositivo a la última condición de trabajo. Además, realiza las opciones de configuración del dispositivo como un administrador en una red donde se necesita un único sistema operativo para la ejecución en todos los dispositivos vinculados.

Una imagen debe incluir el sistema operativo, los controladores del hardware, el programa instalado, las configuraciones, etc. Puedes almacenarla en un sistema de almacenamiento externo debido a su gran tamaño, el uso de una imagen del sistema en un nuevo disco duro y todo ello te permitirá saltarte el proceso de reinstalación

Copa de Seguridad Regular: Una copia de seguridad es una copia de un archivo o carpeta, partición o sector, etc. Suele estar asociada a un único destino de origen la información incluida en una copia de seguridad regular pueden ser cualquier cosa desde archivos multimedia hasta documentos.

Imagen del Sistema v/s Copia de seguridad.

Para ello estableceremos algunas diferencias entre la imagen del sistema y la copia de seguridad regular.

- Velocidad y Espacio de Almacenamiento: Las copias de seguridad y la imagen se usan en un espacio de almacenamiento diferente con una velocidad de transferencia de información variada. Cuando se trata de la velocidad, depende del tamaño del archivo de la copia de seguridad y la eficiencia del hardware del dispositivo. Cuando se ejecuta una copia de seguridad normal se usa menos tiempo que la copia de seguridad del Sistema/Imagen del sistema ya que, pretende centrarse en archivos y carpetas independientes para la realización de la copia de seguridad. Además, una copia del sistema ocupa un mayor espacio de almacenamiento en el disco de comparación con la copia de seguridad en condiciones normales. Por ejemplo, si usas una

unidad de 1Tb y la imagen del sistema ocupa 400 Gb de espació entonces del tamaño de la imagen es de 400 GB, para así evitar el uso excesivo del espacio de almacenamiento.

- Flexibilidad: Cuando se trata de una copia frente a una imagen del sistema, la flexibilidad solo viene con la creación de copias de seguridad regulares. Hay varios archivos en el dispositivo que no son funcionales o no tiene utilidad. Cuando optas por crear una copia de seguridad regular tienes la opción de seleccionar los archivos y carpetas esenciales en la unidad o dispositivo. Pero, en el caso de la imagen del sistema, no tiene otra opción de realizar una copia de seguridad de todo el sistema operativo con todos los componentes funcionales y no funcionales.

- Compatibilidad: Al crear una copia de seguridad se puede crear fácilmente y almacenar el kit en el mismo o en otro dispositivo. Allí es donde aparecen los problemas de compatibilidad, para ello se deben resolverse los errores de compatibilidad para almacenar la copia de seguridad.

- Crear una Imagen del Sistema: Para crear una imagen del sistema hay una utilidad que funciona en Windows, se le conoce como copia de seguridad y restauración. Además, el uso de herramientas de historial de archivo está vinculada a servir, al mismo principio, el de la restauración del sistema. También, se establecen dos soluciones externas el cual describimos en esta sección.

AOMEI Backupper.

Se usa este programa de aplicación a terceros para crear una imagen del sistema, y es el enfoque más accesible. Puedes usar un programa fácil de usar para llevar a cabo el proceso. En esta referencia ayuda crear una Imagen del sistema en poco tiempo, se puede programar las copias de seguridad sobre una base diaria semana o mensual.

SNAP-In.

Además de usar el programa de copia de seguridad de terceros también se usa este aplicativo como complemento del Windows para crear una imagen del sistema. Para ello, también se hará uso de un disco duro externo con una capacidad de almacenamiento de datos.

4. -Disaster Recovery Plan (Plan de recuperación ante desastres informáticos) desde la Nube.

¿Qué es un DRP?

También es conocido como Disaster Recovery Plan (DRP), es un documento donde las empresas describen los procedimientos a seguir para reanudar el área de TI en caso de una interrupción (como caídas de servidores cloud, bases de datos, fallas de

infraestructura o software, catástrofes), y es regido por Disaster Recovery Institute International.

Tipos de DRP.

Al momento de encontrar un método para recuperarse de las contingencias, las empresas optan cada vez más por el DRaaS (Disaster Recovery as a Service) o DRP en la nube. Y si bien, la metodología debe ser la adecuada, es mejor saber la manera de implementarla, para ello hay que saber diferenciar los tipos de formas de recuperación de la información dentro de un modelo de negocio establecido por personal especializado para actuar raídamente y con la idea de minimizar el daño.

- DRP as a Service (DRaaS): El proveedor se encarga tanto el hardware y el software como de su manejo y mantenimiento.
- DRP Usando infraestructura como Servicio: El proveedor vende sus servicios, instalaciones y equipos, pero no se encarga de la instalación, manejo ni mantenimiento.
- DRP usando Backup como servicio: O también llamado datacenter remoto.

Importancia.

Un plan de recuperación ante desastres es determinado e implementado por la empresa para reanudar sus actividades comerciales o de información, en el menor tiempo posible y con el menor impacto en la perdida de los datos. Estos

dimensionamientos deberán ser establecidos previamente en una política general de seguridad con ello se garantizará la respuesta a un incidente. Posteriormente, se establecerá como un documento clave que busque un mínimo de estándar de ciberseguridad, sobre todo con base tecnológica donde la disponibilidad de los sistemas es un asunto crítico.

Su implementación es clave en cualquier proyecto de seguridad ya que su aplicación asegura la continuidad de las empresas, esta es una de las principales razones por la que un regulador o cliente corporativo se le solicitará en la auditorías establecidas para ello.

EL DRP limita los pasos a seguir para restaurar la tecnología rápidamente y hacer que los sistemas estén disponibles en situaciones extremas de desastre. También se deben definir los valores de las métricas RPO (Tiempo en que ocurre la pérdida real de los datos) y RTO (Tiempo que lleva a solucionar el incidente). El Recovery Point Objetive (RPO) y Recovery Time Objective (RTO) son dos métricas de tiempo imprescindibles para el plan de recuperación y que ayudan a crear estrategias que sean posibles aplicar para el negocio.

- RPO (Recovery Point Objective): Es el tiempo máximo aceptable que puede transcurrir entre el momento en que se ha realizado la última copia de seguridad de los datos y un incidente. Para que un valor sea ínfimo debes realizar gran cantidad de Backups, y eso implica mayores costos en los proveedores. Por lo general, las empresas establecen como máximo el SLA (acuerdo de nivel de servicio) por ejemplo de 24 horas.

- RTO (Recovery Time Objective): Es el tiempo que un negocio necesita para recuperar los servicios después de producido el incidente. Para ello, se establecerá como métrica el tiempo de restauración que tengas con tu proveedor de la nube y cuánto demora en levantar los servicios caídos. Generalmente, se dan entre 4 y 8 horas, aunque dependerá de la dificultad de lo instalado.

Como se realiza un DRP.

PLANIFICACIÓN DE LA RECUPERACIÓN: Las causas por las que una empresa generalmente no recupera más que el 31% de los datos se debe a la ausencia de un plan en el que se especifiquen los pasos a seguir. En caso de contingencia, los servidores de DRP deben de funcionar en forma correcta.

ESTABLECER LA IMPORTANCIA DE LOS DATOS: Con un análisis de los procesos mínimos que una empresa requiere para operar, se podrá determinar qué es lo más importante para que la empresa siga funcionando. Para ello, se establecerá una jerarquización de los datos y lo niveles de importancia.

DESARROLLO DE UN SIZENING EFECTIVO: Simplemente funcionando el DRP se sabe que funcione como un espejo dentro de la organización que se tiene habitualmente la realidad. Ubicados los procesos más importantes se establecerá posteriormente un adecuado Sizeing que posibilite a la empresa trabajar con lo mínimo.

DETERMINAR UN RÉGIMEN PARA EL BACKUP: Si bien la recomendación es que el backup de imágenes sea periódico, cada organización preverá cómo será la operación más efectiva en la operación de recuperación y, además, es imprescindible comprobar que el Backup funciones correctamente.

LA NUBE NO LO ES TODO: Actualmente, la nube surge como una alternativa menos costosa, sin embargo, también es recomendable complementar el almacenaje de Backup con un servidor storage local.

ESTABLECER NORMAS DE SEGURIDAD: De acuerdo con las políticas de seguridad establecidas en la organización y que efectivamente se cumplen, y se elaboren la normas que el proveedor también debe cumplir.

CAPACITACIÓN FRENTE A LAS CONTINGENCIAS: Cada colaborador dentro de la organización debe ser informado de su actuación frente a un incidente. Por ello, se establecerán capacitaciones en donde se indique el procedimiento, y, es necesario crear una red de comunicación y de secuencia para el proceso de la contingencia.

COMPROBACION DE QUE EL DRP FUNCIONA: Es imposible disponer la capacitación sin comprobar si el sistema funciona, por lo que es necesaria tener planificadas varias pruebas que pueden ir escalonadas en función del tamaño de los conflictos.

COMPLEMENTOS DEL DRP: Además de la tecnología para su implementación, se deben tener en cuenta los planes elaborados de manejo de crisis que forman parte del BCM (Business Continuity Management), y que colaboran en la conformación de su empresa.

ANALISIS DE RECURSOS: La implementación de un DRP es una tarea compleja, que no solo requiere esfuerzos, sino también tiempo y manos que lo puedan llevar a cabo, controlar y evaluación constante. Es por ello, que es necesario el análisis con sinceridad respecto a cuantos recursos de su empresa serán utilizados en la prevención de desastre, para que abogue en su productividad y en la seguridad de ésta.

Consideraciones para la copia de seguridad como un servicio.

Para las organizaciones que están luchando con un producto de Backup legado, donde cualquier tipo de actualización probable sea un reemplazo significativo, el respaldo como servicio (Backup as a Service o BaaS) puede ser una buena opción. Realizan respaldo de la información, copias de seguridad, los productos BaaS también proporcionan agilidad por que los datos son accesibles de forma nativa o se pueden recuperar desde el proveedor de la nube.

La recuperación de la Nube.

Para las organizaciones cuyo servicio de recuperación y la copia de seguridad están basados en modelos BaaS no necesariamente es la mejor respuesta. En cambio, la mayoría de los productos de respaldo tienen la oportunidad de almacenamiento basado en la nube:

- Los agentes de copia de seguridad existentes en los servidores se mantienen intactos.

- Los trabajos y las planificaciones de copia de seguridad existentes continúan operando sin afectaciones.
- La capacidad de recuperación desde el almacenamiento local no disminuye.
- Una Copia terciaria de la copia de seguridad de la información establecida en un repositorio en la Cloud para fines de cumplimiento.

Mientras parece fácil su implementación, puede ser compensado usando los medios por los que se replican los datos desde el servidor de copia al repositorio de la nube. También, se puede presentar una afectación drástica a la agilidad y la recuperación de las opciones de copia de la nube.

Planeamiento de una Arquitectura Híbrida o D2D2C.

La mayoría de las organizaciones mantienen con dificultad los acuerdos de nivel de servicio en los tiempos de recuperación. Debido a esto, se recomienda que la mayoría de productos de respaldo y recuperación sean configuraciones "D2D2C" del disco de producción a los discos de respaldos locales (D2D), antes de ir a la Cloud (2C). Dicho esto, D2D2C puede tener varias permutaciones:

- Productos BaaS con un producto intermedio de almacenamiento en caché antes de ir a los repositorios BaaS.
- Hardware de respaldo en las instalaciones que realice las copias a otra instancia de Software con un proveedor de servicio.
- Software de respaldo en las instalaciones que realice la copia de seguridad a otra instancia de software con un proveedor de servicio.

- Software de respaldo en las instalaciones que grabe en un repositorio de almacenamiento en la nube como nivel superior.

LA NUBE NO DESTRUYE LA CINTA.

Esto ocurre mientras otras tecnologías innovadoras de TI usurpan un cierto uso de la cinta. No necesariamente D2D2C es un sustituto adecuado de D2D2T (la cinta) debido a la incapacidad o la falta de voluntad de la mayoría de los proveedores para conservar los datos 10 o 15 años.

NUBE Y VIRTUALIZACIÓN = RECUPERACIÓN DE DESASTRES.

La virtualización hace que los servidores de producción sean más portátiles y la infraestructura de nube (que proporciona ubicación secundaria de manera económica) puede permitir la recuperación de desastres en forma rudimentaria. Esto es solo a las empresas medianas, sin embargo, las empresas grandes tienen otras opciones.

COPIA DE SEGURIDAD EN SaaS.

Se usan los servidores de producción para este tipo de recursos, de tal manera, que muchas cargas de trabajo se mueven a la nube. Incluyendo la plataforma de correo electrónico, los sistemas CRM como Salesforce y el intercambio de archivos.

Desafortunadamente, muchos productos SaaS aún no han desarrollado las API para ampliar la cobertura de respaldo empresarial para las plataformas SaaS. Estas API se crean conforme las plataformas crecen en el uso del flujo principal sin estas APIs, los desarrolladores tradicionales de Backup han sido lentos para agregar otras ofertas de SaaS.

PROTECCION DE LOS DATOS.

Un tema importante que se debe cuidar en una organización es la seguridad en la red informática. Por lo que hay diferentes dispositivos interconectados y existe la posibilidad que uno de ellos pueda llegar a afectar a los demás si no se cuenta con una protección eficaz. La protección de las Redes implica una COPIA DE SEGURIDAD CENTRALIZADA, la cual debe realizarse de forma periódica en un espacio de tiempo determinado por un estudio previo de preferencia en un espacio completamente diferente.

Es importante darle un mantenimiento adecuado y oportuno a las redes, pues con el tiempo pueden llegar a ser vulnerables y el riesgo aumenta. Contar con una seguridad de las redes garantizara su funcionamiento.

CONSOLIDACION DE LOS EQUIPOS EN UN SOLO NIVEL.

Unos de los problemas actuales con el uso de este tipo de almacenamientos, es el uso excesivo de energía eléctrica y altos costos de mantenimiento. La forma de reducir estos costos es a través de la Virtualización de los Servidores, un servicio que se adapta a las necesidades del negocio además de reducir drásticamente el espacio en la infraestructura.

Unifica tecnología con IIOT.

En los últimos años, el Internet Industrial de las Cosas ha comenzado a tener un impacto directo en la economía de los países. El Internet de las Cosas es una tendencia tecnológica que implica la integración entre las cosas que nos rodean a las personas y a las empresas en todos los ambientes. Permite a la infraestructura vincular a los objetos con las redes de comunicación al habilitar datos que nunca antes habían estado disponibles.

Esta tendencia tecnológica que adoptan las industrias para la operación Inteligente de las máquinas, computadoras, robots, teniendo como objetivo la optimización de los servicios y producción.

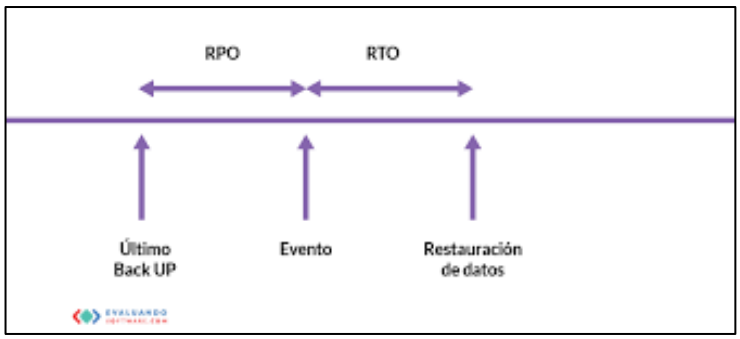
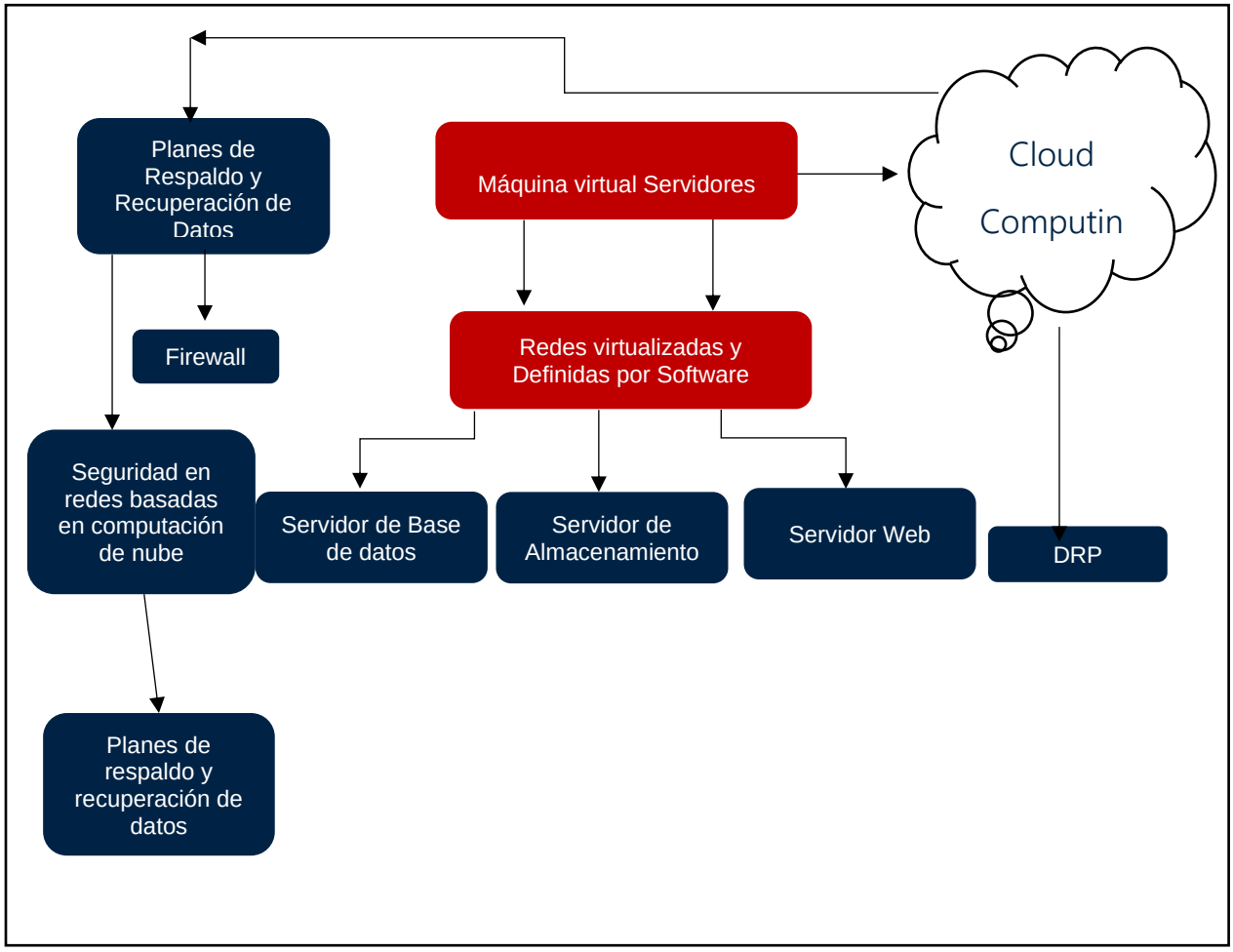


Figura 1: DRP

Extraído de: http://i.imgur.com/nE91GxE.png

Cierre

Por medio del siguiente organizador gráfico, se destacan las ideas clave de esta semana: Seguridad de Almacenamiento en el Datacenter.



¿Qué es una copia de Seguridad?

En el sentido más académico, una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos. Una medida indispensable para garantizar su continuidad y conservar la confianza que nuestros clientes han depositado en nuestra organización. De lo contrario, podríamos proyectar una imagen negativa y generar desconfianza.

Referencias bibliográficas

U.S.A.: TIA, 2005 TIA Standard: Telecommunications Infrastructure Standard for DataCenter; ebooks

https://manuais.iessanclemente.net/images/9/9f/Tia942.pdf

Mark A. Sportack, Pearson Educación, 2003 - 354 páginas Fundamentos de enrutamiento IP

Abts, Dennis. High performance datacenter networks: architectures, algorithms, and opportunities ISBN: 9781608454020

https://bit.ly/3oqlVSL

Gutiérrez (2019).