UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

Desarrollo del correcto control de respaldo de información para usuarios finales con Acronis Management.

T E S I S

Para obtener el título de:

LICENCIADO EN INFORMÁTICA

P R E S E N T A :

JOSÉ ALFREDO HERNÁNDEZ DE ANDA

Asesor: M.A. Aurora Reyes Vigueras

CUAUTITLÁN IZCALLI, ESTADO DE MÉXICO, 2022

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

VNIVERSIDAD NACIONAL AVTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN
SECRETARÍA GENERAL
DEPARTAMENTO DE TITULACIÓN

U. N. A. M.

ASUNTO: VOTO APROBATORIO

DR. DAVID QUINTANAR GUERRERO
DIRECTOR DE LA FES CUAUTITLAN
PRESENTE

ATN: DRA. MARÍA DEL CARMEN VALDERRAMA BRAVO
Jefa del Departamento de Titulación
de la FES Cuautitlán.

Con base en el Reglamento General de Exámenes, y la Dirección de la Facultad, nos permitimos comunicar a usted que revisamos el: **Trabajo de tesis.**

Desarrollo del correcto control de respaldo de información para usuarios finales con Acronis Management

Que presenta el pasante: **José Alfredo Hernández de Anda**
Con número de cuenta: **415098265** para obtener el título de: **Licenciado en Informática**

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el **EXAMEN PROFESIONAL** correspondiente, otorgamos nuestro **VOTO APROBATORIO**.

ATENTAMENTE
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cuautitlán Izcalli, Méx. a 09 de septiembre de 2022.

PROFESORES QUE INTEGRAN EL JURADO

	NOMBRE	FIRMA
PRESIDENTE	Mtro. Ing. Elect. Gerardo Vigil Sanabria	
VOCAL	M.A. Aurora Reyes Vigueras	
SECRETARIO	L.S.C. Liana López Pacheco	
1er. SUPLENTE	L.I. Elizabeth Barrera Romero	
2do. SUPLENTE	Lic. Hector Adrián Vega Becerril	

NOTA: los sinodales suplentes están obligados a presentarse el día y hora del Examen Profesional.

MCVB/ntm*

Agradecimientos.

Agradezco a mi familia los pilares de mi vida, los cuales me han apoyado en cualquier decisión de mi vida y no rendirme ante las malas decisiones.

A mi madre Socorro, la cual fue la persona que nunca se rindió y siempre estuvo impulsándome al estudio, confiando en mí y regañándome lo necesario para ser un mejor alumno.

A mi padre José Hugo, el cual siempre me dio buenos consejos de la vida, por siempre preparar mis almuerzos o comidas de la escuela y a pesar de no tener dinero siempre me apoyabas hasta con el último centavo de tu cartera.

Gracias a mis padres por la mejor herencia del mundo “mis estudios”.

A mi hermano Hugo por mostrarme el mundo de la informática ser mi apoyo y enseñarme ser autónomo, gracias por ser mi admiración y ejemplo para seguir.

Agradezco a la Universidad Autónoma de México, por dejarme vestir y representar sus colores azul y dorado.

Agradezco a mi segunda casa, la Facultad de Estudios Superiores Cuautitlán, la cual me acogió con un gran abrazo y me permitió ejercer mi carrera profesional dentro de sus instalaciones, otorgándome grandes herramientas para crecer personal y profesionalmente.

A mi asesora, M.A Aurora Reyes Vigueras que me ayudó mucho, que me esperó, me dio miles de valiosos consejos, me otorgó su valioso tiempo incluso fines de semanas con el fin de poder mejorar el presente trabajo. Gracias por su gran profesionalismo.

Agradezco a mi honorable jurado por su valioso tiempo, los cuales me ayudaron y comprendieron mi situación laboral para mejorar la presente tesis.

Agradezco a mi mejor amigo Ricardo Barahona por sus años de amistad y me ha impulsado para llegar a estos momentos de mi vida, agradezco a mi amigo Arturo Rocha el cual siempre me impulso con sus consejos y risas.

Agradezco a todos mis compañeros de trabajo en especial a Sergio, compañero de trabajo el cual me impulsó y me enseño mucho sobre el mundo de sistemas, a Mario y Héctor los cuales me enseñaron el mundo de redes y el cableado estructurado.

Índice

Introducción

Hoy en día, la información es importante en las pequeñas y grandes empresas, de tal modo que siempre se requiere de la misma en cualquier momento. Ya sea información relevante, rápida o de consulta, toda esta información es almacenada en dispositivos tecnológicos por ejemplo Laptops, Computadoras de Escritorio, Dispositivos Móviles, etcétera.

Estos dispositivos tecnológicos almacenan grandes cantidades de información día a día, por lo cual es importante mantener resguardada y segura la información. Sin embargo, estos problemas de seguridad son comunes como es el robo de esta o en el peor de los casos, la pérdida de información.

Por otro lado, los usuarios finales no tienen interés de resguardar su información, como son datos personales o información delicada de la empresa, tampoco tienen el interés de ser precavidos al realizar sus actividades no laborales mientras operan la información de la empresa u organización, realizan otras actividades como navegar en internet o descargar algún tipo de archivo multimedia.

Estos huecos de seguridad pueden ser corregidos con capacitaciones o pláticas con los usuarios finales, en algunas empresas estas prácticas pueden ser consideradas como pérdida de tiempo, por lo cual el usuario final se define como el eslabón más débil de una cadena de seguridad de información.

Por lo tanto, en una empresa u organización se necesita resguardar toda la información de cada usuario o dispositivo tecnológico, cualquier información que está resguardada en un archivo es importante y útil. Existen diversos sistemas de respaldo pueden ser de paga o gratuitos.

En este trabajo se mostrará la forma de cómo se implementa el correcto desarrollo del control de respaldos con Acronis Management para usuarios finales.

Acronis se ha convertido en una opción para el almacenamiento en el Cloud Híbrido para pequeñas o grandes empresas. A través de soluciones innovadoras de seguridad, recuperaciones de información ante desastres o protección activada

basada en IA (Inteligencia Artificial). A estas funciones de Acronis se les sacará provecho mediante el uso correcto de control de la consola de respaldos, se conocerá profundamente la consola y cómo configurarla correctamente, de tal modo que se logrará tener un sistema de respaldo de información Inteligente y Autónomo.

Planteamiento del problema

Actualmente las empresas mexicanas tienen una pérdida de información diaria de 2.13 Terabytes según el economista, periódico especializado en finanzas y mercado, en una escala de 0% al 100%, en las organizaciones mexicanas el 28% de las organizaciones fueron objeto de un ataque Ransomware, 15% sufrió un desastre local lo cual afectó el acceso a su información y el 12% no pudo recuperar su información con el sistema de respaldos que maneja. Si se compara con el 45% de las organizaciones que dijo haber experimentado tiempo de inactividad en su sistema de respaldo o ni siquiera tener planificado la implementación de algún sistema de respaldo de información, por lo tanto, la pérdida de información es crítico en las organizaciones mexicanas.

Hipótesis

Si se lleva a cabo un correcto control del agente de respaldos de información, entonces se tendrá un mejor control de la información en la organización y no se sufrirían pérdidas o robo de información.

Justificación

Debido al mal control de respaldo de la información, se tiene la necesidad de implementar un plan de respaldos, como es el Agente de Acronis Management el cual contiene los procesos necesarios para solventar el problema actual de las empresas mexicanas y esto permitirá tener un correcto control de información y respaldo de está.

Objetivos de la Investigación

Desarrollar una propuesta de un sistema de respaldo autónomo en una organización y cómo realizar su correcta implementación.

- Explicar la importancia de la pérdida de información.
- Comprender los tipos de pérdida de información.
- Conocer las diferentes formas de respaldar la información.
- Diseñar el proceso de implementación de Acronis Management.
- Desarrollar el proceso del correcto control del agente de Acronis Management.

Capítulo 1. El equipo de cómputo

Tiempo atrás se manejaba la información con documentos, carpetas, archiveros, etcétera. Este manejo antiguo de información provocaba un gran volumen de espacio para almacenarlo, el cual era de gran dificultad realizar una búsqueda de un archivo en específico. Conforme el tiempo pasa, la tecnología ha avanzado día tras día, dejando atrás las gestiones antiguas del manejo de datos y para esto llegó el “Equipo de Cómputo o Computadora”.

Se puede mencionar maravillas del equipo de cómputo, por ejemplo, la optimización de sus procesos, este logro llevo que grandes cantidades de información puedan estar en la palma de la mano y de que igual forma se pueda realizar búsquedas de información inteligentes. Pero antes de seguir mencionando las maravillas del equipo de cómputo debemos de saber realmente ¿Qué es un Equipo de Cómputo? ¿Cómo funciona? y ¿Cómo se compone?

1.2 ¿Qué es un equipo de cómputo?

En primera instancia se debe de conocer lo que significa cada palabra, según la real academia española “Equipo” significa: “Conjunto de aparatos constituido por una computadora y sus periféricos”. También el diccionario menciona que “Computo o Computar” significa: “Contar o calcular en número algo, principalmente los años, el tiempo o la edad.”

Según Juan Bernardo Vázquez Gómez en su libro de Arquitectura de Computadoras 1, la definición de un Equipo de Cómputo es la siguiente: “Un computador o computadora es una máquina calculadora electrónica rápida que acepta como entrada información digitalizada, la procesa de acuerdo con una lista de instrucciones almacenada internamente y produce la información de salida resultante. A la lista de instrucciones se le conoce como programa y el medio de almacenamiento interno memoria del computador”.

Por lo que se llega a la conclusión de que un equipo de cómputo es un dispositivo electrónico capaz de procesar, almacenar y visualizar datos por medio de instrucciones, las cuales permiten que el usuario final pueda gestionar y procesar una gran cantidad de información.

1.3 Estructura de un equipo de cómputo

Según Juan Bernardo Vázquez Gómez en su libro de Arquitecturas de Computadoras 1 dice que “La computadora se conforma por dos elementos principales: hardware y software. El hardware se refiere a la parte física de la computadora: teclado, gabinete circuitos, cables, discos duros, impresoras, monitores, etcétera. El funcionamiento del hardware depende del software (programas). En tanto que software lo define como el conjunto de instrucciones que dirigen al hardware. Asimismo, dice que es un conjunto de instrucciones que realizan una tarea específica denominada programa.”

Patricia Quiroga menciona que “Una computadora es un sistema que incluye módulos de hardware y de software. El hardware es el conjunto de dispositivos electrónicos y electromecánicos que constituyen la estructura física de la computadora. Sin el software, el hardware no podría procesar dato alguno o quedaría limitado a una tarea fija, como se menciona en procesadores de propósito específico. Un término más, que involucra ambos conceptos, es firmware y se utiliza para identificar los dispositivos físicos programados, como puede ser la programación de los múltiples usos que presta un electrodoméstico, o sea, que se fusionan los conceptos de hardware y software.”

Se puede concluir que un Equipo de Cómputo se estructura en dos elementos importantes que son.

- Hardware

El hardware son todos los elementos físicos que componen a la computadora, aunque existen dos tipos de Hardware, uno elemental y otro complementario.

- Hardware Elemental son los dispositivos electrónicos que son vitales para que funcione el equipo de cómputo, por ejemplo: MotherBoard (Tarjeta Madre), Procesador, Memoria RAM, Disco Duro, etcétera.
- Hardware Complementario son los dispositivos electrónicos opcionales que se pueden agregar a nuestro equipo de cómputo y nos proporcionan servicios adicionales, por ejemplo: Impresoras, Scanner, Bocinas, Monitor, Mouse, Teclado, Cámara Web, etcétera.

Software

El software son todos los programas que permiten procesar y almacenar datos o información por medio de una serie de instrucciones dirigidas hacia el ordenador (equipo de cómputo), existen dos tipos de software en los cuales en esta ocasión se enfocará al software de código abierto y software de paga, ya que es el tipo de software que se encontrará para la gestión y proceso de la información.

- Software de código abierto, consiste en un programa realizado sin fines de lucro el cual siempre es gratuito y el código del software abierto al mundo para realizar modificaciones al programa.
- Software de paga, consiste en programas de paga el cual te dan un periodo de 30 días para probarlo completamente para finalmente ofrecer el producto final, normalmente estos programas contienen un soporte proporcionado por la empresa que realizo el software.

1.4 Importancia de un equipo de cómputo

Hoy en día el equipo de cómputo es indispensable tanto en la vida cotidiana como el ámbito laboral. Un equipo de cómputo ofrece optimizar procesos, gestionar grandes volúmenes de información, realizar búsquedas rápidas, etcétera.

Es importante tener en cuenta que la tecnología avanza día a día por lo cual existen miles de herramientas virtuales para realizar cualquier tarea y así poder optimizar cualquier proceso que queramos.

1.5 Tipos de equipo de cómputo

Es necesario conocer importancia de los diferentes tipos de equipo de cómputo, ya que al momento de que se arme un ordenador existen diferentes configuraciones para el funcionamiento real de la computadora, es decir que existen diversos hardware que proporcionan diferentes compañías para poder armar un equipo de cómputo.

Según la autora Patricia Quiroga y la Universidad Complutense de Madrid, enlista los siguientes tipos de equipo de cómputo:

1.5.1 Workstation

Una Workstation (Equipo de Trabajo) es una computadora compacta que se encuentra conectada a un dominio de red local, estas computadoras tienen un rendimiento un poco mayor a las computadoras personales, ya que están optimizadas para la manipulación de diferentes tipos de datos y estar encendidas en jornadas laborales largas.

Normalmente las Workstation son los equipos que se compran exclusivamente para el manejo de datos o información para las empresas convencionales, son computadoras con un rendimiento un poco mayor a los Ordenadores de Escritorio, pero lo que lo diferencía a los demás es su largo rendimiento por largos periodos de actividad.

1.5.2 Súpercomputadoras

Continuando con la Universidad Complutense, Una supercomputadora también se le puede denominar como "Superordenador" es un equipo con una capacidad alta de realizar cálculos muy superiores a los ordenadores comunes, el

precio de este equipo es elevado y está limitado a ciertos tipos de organizaciones, ya que es utilizado por militares, organizaciones gubernamentales, instituciones educativas y empresas. Según el sitio web mexicano especializado en tecnología Xataka, existen 500 súpercomputadoras en todo el mundo, de las cuales China tiene 219.

Los usos más comunes de las súpercomputadoras son: predicción del clima, animaciones complejas 3D, cálculos de fluidos dinámicos, investigación nuclear, exploración petrolera, etcétera.

1.5.3 Mainframe

Citando nuevamente a la Universidad Complutense, *un mainframe, de igual forma que una supercomputadora, es un ordenador con capacidades altas, pero no tan altas como ésta, ya que un mainframe y una supercomputadora pueden tener características iguales, pero no son lo mismo. Los mainframes están enfocados en procesar una gran cantidad de datos o soportar una gran cantidad de usuarios conectados al mismo tiempo. Los mainframes tienen la característica de poder arreglarse sin dejar de funcionar, por lo cual tienen la capacidad de estar prendidos durante años.*

1.5.4 Ordenador de Escritorio

También conocido como Desktop, el ordenador de escritorio está diseñado para ser utilizado en un escritorio en una oficina o en un hogar, en esta categoría normalmente su configuración es básica, aunque un Ordenador de escritorio te da la posibilidad de aumentar el nivel de proceso de este.

1.5.5 Laptop

Equipo portátil que sustituye al ordenador de escritorio ya que tiene la ventaja de poder portar el equipo a cualquier lado y tener las mismas funciones que un ordenador de escritorio. Tiene muchas de alternativas a la hora de adquirirlas y es recomendable saber el uso que se le dará, ya que las posibilidades de mejorar el equipo son muy limitadas.

Capítulo 2. La información y la importancia de su almacenamiento

2.1 Concepto de la información

Según Idalberto Chiavenato, la Información “Es un conjunto de datos con un significado, o sea que reduce la incertidumbre o que aumenta el conocimiento de algo.”

La información es un conjunto de datos seleccionados y ordenados con un propósito específico para poder generar un conocimiento de algo.

2.1.1 Tipos de información

Es necesario conocer la información que se puede manejar en una organización, aunque se tenga el concepto de que la información es valiosa y debe de estar resguardada. También se le debe de dar prioridad al tipo de información que se maneja, no se le debe de dar el mismo tratamiento a una información Confidencial, la cual se restringe el acceso a los usuarios, que, a una información Pública, en la cual todos los usuarios tienen permiso de visualizar.

Según los apuntes de la materia de Informática, publicada en línea por la Facultad de Contaduría y Administración de la Universidad Nacional Autónoma de México existen dos tipos de información:

2.1.1.1 Información Interna

Las fuentes de información interna son todas aquellas que la empresa puede obtener y explorar por sus propios medios, por ejemplo, permiten obtener información referente a los clientes, los estados financieros que muestran su

situación financiera, los registros de inventarios, de ventas, de costos, el personal de la empresa.

2.1.1.2 Información Externa.

La tecnología ha permitido que las empresas puedan reunir, archivar y evaluar la información, por ejemplo, para la auditoría externa: Las fuentes de información inédita incluyen encuestas de clientes, investigaciones de mercados, discursos en juntas de accionistas y profesionales, programas de televisión, entrevistas y conversaciones con diversas partes interesadas. La información estratégica, además de los índices, las bases de datos en línea permiten encontrar información en cientos de publicaciones, por tema, industria, nombre de la organización, número de clasificación industrial (NCI), tipo de producto, zona geográfica o tipo de publicación. La insatisfacción de los consumidores continúa porque la gerencia carece de la información adecuada acerca de los planes de mercadotecnia. Es posible que la empresa no advierta que su producto no cumple con las expectativas de sus consumidores.

2.1.2 Importancia de la información

Hoy en día la cantidad de información que es creada, modificada y enviada, es inmensa, es vital tomarle suma importancia la información que se maneja en una organización como la información que manejamos personalmente.

Para esto es necesario conocer la diferencia de estas mismas.

2.1.2.1 En una Organización

La información en una organización es importante, ya que se encuentra actualizándose a diario por trabajadores activos, por lo tanto, si un documento interno de suma importancia llega a ser eliminado por error y el departamento funciona con base en la información pérdida, el impacto de la pérdida de información en el departamento es grande.

2.1.2.2 Personal

Normalmente cuando se lee información personal se piensa en, música, fotos, videos, etcétera., este tipo de información es normal para un usuario ya que la maneja a diario, pero realmente la información personal se refiere a la dirección de domicilio, Registro Federal de Causantes, CURP (significado), Cédula Profesional, Datos Bancarios, Firmas, Número de Teléfono, etcétera.

El objetivo principal de un Hacker (usuario final que tiene como objetivo el robo de la información) es la información personal que resguarda una organización, principalmente en los Bancos, por lo tanto, es importante tener resguardado la información personal de los usuarios en una organización.

2.2 Almacenamiento de datos

Según HPE (Hewlett Packard Enterprise) Organización especializada en almacenamiento de datos el almacenamiento de datos es: “El almacenamiento de datos se refiere al uso de medios de grabación para conservar los datos utilizando PC y otros dispositivos. Las formas más frecuentes de almacenamiento de datos son el almacenamiento de archivos, el almacenamiento en bloque y el almacenamiento de objetos, cada uno de los cuales resulta adecuado para un fin diferente”.

2.2.1 Tipos de Almacenamiento

Según Red Hat empresa experta en TI define 5 tipos de almacenamiento.

2.2.2 Almacenamiento de Datos

El almacenamiento de datos es el proceso mediante el cual la tecnología de la información archiva, organiza y comparte los bits y bytes que conforman los sistemas de los que dependemos todos los días, desde las aplicaciones hasta los protocolos de red, los documentos, el contenido multimedia, las libretas de direcciones y las preferencias del usuario. Es un elemento fundamental del big data.

2.2.2.1 Almacenamiento definido por software

El almacenamiento definido por software (SDS) es, por una parte, un software de virtualización y, por otra parte, un software de gestión de almacenamiento. Extrae los bits y los bytes de los datos del hardware, formatea los datos en bloque, objeto o archivo, y los organiza para el uso de la red.

El SDS funciona particularmente bien con cargas de trabajo basadas en datos no estructurados (como los sistemas de almacenamiento de objetos y bloques de los que dependen los contenedores y los microservicios), ya que puede expandirse a un nivel que no alcanzan las soluciones de almacenamiento conectadas.

2.2.2.2 Almacenamiento en la nube

Cuando un software de gestión y automatización virtualiza y coordina el almacenamiento, que antes era un recurso físico, se convierte en almacenamiento

en la nube. Esta descripción tiene algunos matices (el recurso debe estar disponible por solicitud a través de portales de autoservicio que sean compatibles con el escalamiento automático y la asignación dinámica de recursos), pero la virtualización, la gestión y la automatización son los tres elementos fundamentales de cualquier recurso en la nube, incluido el almacenamiento.

Actualmente las organizaciones están mudándose al almacenamiento en la nube, porque a pesar de que es accesible y práctico, la seguridad que te da la organización que le contratas este servicio es un poco más elevada a la que comúnmente las organizaciones llegan a aplicar.

2.2.2.3 Almacenamiento adjunto en la red.

Citando de nuevo a Red Hat, el almacenamiento conectado a la red (NAS) es una arquitectura de almacenamiento que facilita el acceso a los datos dentro de una red. Se instala un sistema operativo simplificado en una caja de hardware tan sencilla como un servidor común y corriente: con discos duros, procesadores, memoria de acceso aleatorio y todo lo demás.

Esta caja (conocida como caja de NAS, servidor de NAS, puerta de enlace de NAS o unidad de NAS) se ocupa de todas las funciones de almacenamiento, organización y uso compartido de datos de toda la red.

El almacenamiento NAS, facilitado por protocolos de transferencia que permiten compartir datos entre dispositivos, procesa las solicitudes de almacenamiento de toda la red, lo cual ofrece a la empresa un mejor desempeño, una mayor accesibilidad y más tolerancia a fallos en una única solución fácil de instalar.

2.2.2.4 Almacenamiento de Objetos

Un objeto es una parte de los datos vinculada con los metadatos relacionados, que proporcionan un contexto sobre los bytes de dicho objeto (por ejemplo, la antigüedad o el tamaño de los datos). Los datos y los metadatos conforman el objeto. Los datos almacenados en los objetos no están comprimidos ni cifrados, y los objetos en sí se organizan en almacenes (repositorios centrales con muchos otros objetos) o contenedores (paquetes que contienen todos los archivos necesarios para que se ejecute una aplicación). La organización de los objetos, los almacenes y los contenedores es plana, en comparación con la estructura jerárquica de los sistemas de almacenamiento de archivos, lo cual permite acceder a ellos rápidamente y a gran escala. El almacenamiento de objetos y los contenedores van de la mano: los contenedores se migran de los entornos sin sistema operativo a las máquinas virtuales, y las nubes privadas se migran a nubes públicas, lo cual generalmente se realiza para que los sistemas de almacenamiento logren la capacidad necesaria. Es difícil migrar el almacenamiento tradicional, y el almacenamiento de archivos se torna complejo para la navegación al nivel del petabyte, pero los objetos contienen la información suficiente para que una aplicación la encuentre rápidamente, y el espacio suficiente para almacenar datos no estructurados, como las imágenes y los archivos de texto.

2.2.3 Unidad de almacenamiento.

Según el Manual de Procedimiento de Dispositivos de Almacenamiento y Transportación de Datos publicado por la Facultad de Medicina Veterinaria y Zootécnica, de la Universidad Nacional Autónoma de México “son dispositivos periféricos del sistema, que actúan como medio de soporte para la grabación de programas de usuario, así como de datos y ficheros que son manejados por las aplicaciones que se ejecutan en estos sistemas.”

Por lo tanto, las unidades de almacenamiento son los periféricos que resguardan los datos o información que se le ordenará a la computadora.

2.2.3.1 Tipos de dispositivos de almacenamiento

Existen tres tipos de almacenamiento, Magnético, Óptico, Memorias de Estado Sólido y Almacenamiento en Nube, es necesario conocer los tipos de almacenamientos existe y se pueden utilizar a la hora de realizar un respaldo de información desde el punto de vista informático.

Según la Universidad Politécnica de Valencia son los siguientes:

2.2.3.1.1 Magnético

Los dispositivos magnéticos usan partículas cargadas sobre una superficie para almacenar la información, en función de su orientación, representan un cero o un uno. Los dispositivos cuentan con un cabezal de lectura/escritura que es un imán que se encarga de orientar las partículas al escribir o de determinar su posición al leer.

2.2.3.1.1.1 Cinta Magnética

Los primeros dispositivos magnéticos empleados fueron las cintas. Es un dispositivo capaz de almacenar grandes volúmenes de información en un espacio muy pequeño a un coste muy bajo. Su principal inconveniente es que el método de acceso a los datos es secuencial. Esto quiere decir que, para acceder a un dato que se encuentre en cualquier posición de la cinta antes hemos tenido que leer todos los datos anteriores.

2.2.3.1.1.2 Disquete o Floppy Disk

Los disquetes o floppy disk fueron los primeros discos usados en los ordenadores personales. Son una pieza de material magnético flexible cubierta por una capa de plástico a modo de sobre, rígida o semirrígida. Para su lectura, los ordenadores disponen de una unidad para leer y escribir contenidos en ellos, denominada disquetera. El tamaño de los disquetes indica su diámetro en pulgadas. Se popularizaron en dos tamaños principalmente:1 discos de 5,25", con una capacidad de 360 kb (si, has leído bien, menos de medio megabyte) y discos de 3,5", con una capacidad de 720 kb o finalmente de 1,44 Mb. Actualmente, la mayoría de los ordenadores personales ya no incluyen disqueteras de serie y los únicos vestigios que quedan es el botón para encendido y apagado.

2.2.3.1.1.3 Disco Duro (HDD)

El dispositivo magnético por excelencia hoy en día es el disco duro y todos los ordenadores incorporan al menos uno. Está formado por una pila de discos rígidos metálicos magnetizados en cuyas superficies se almacena la información. Esta pila de discos se encuentra encerrada en una carcasa metálica para protegerla del exterior (la más mínima mota de polvo puede inutilizarlos). La capacidad de los discos actuales se mide en terabytes (Tb).

2.2.3.1.2 Óptico

Los discos ópticos emplean una luz láser en lugar de un imán para leer y escribir bits de datos en una capa reflectante. Esta capa está protegida por una superficie de plástico transparente que permite que la luz pase. La capacidad de los discos ópticos varía en función de su tipo y del número de capas de datos que

contengan. La velocidad de lectura y de escritura depende del dispositivo lector/grabador

2.2.3.1.2.1 CD

Los primeros medios ópticos empleados fueron los CD-ROM (Compact Disc-Read Only Memory). Son discos de sólo lectura, que sólo se pueden escribir una vez. Emplean la misma tecnología que los CD de audio. De hecho, las especificaciones técnicas de los distintos formatos están publicados en una serie de libros identificados por colores, entre los que tenemos:

- *Libro rojo CD-DA (compact disc-digital audio): son los discos de música*
- *Libro amarillo CD-ROM: discos compactos de sólo lectura*
- *Libro naranja CD-R y CD-RW: discos compactos grabables y regrabables.*
- *Libro blanco VCD: disco de vídeo, antecesor del DVD (e incompatible con él)*

2.2.3.1.2.2 DVD

En el caso de DVD, tenemos una gran variedad de formatos. Inicialmente, aparecieron los formatos generados para la distribución de contenidos por parte de la industria en DVD de vídeo o, menos habituales, de audio. Estos discos, al igual que ocurre con los CD, son discos de solo lectura y se denominan DVD-ROM. Para los discos de datos (grabables) aparecieron varias opciones excluyentes e incompatibles entre sí: se trata de los DVD-RAM, los formatos -R y los +R.

2.2.3.1.2.3 Blue-Ray

Un nuevo movimiento en la industria hacia formatos de alta definición y el intento de mejorar la protección de los contenidos7 hizo aparecer dos formatos: HD-

DVD (Toshiba) y Blu-Ray (Sony). El formato de DVD-Video tiene una resolución máxima de 720 píxeles (en horizontal) y para el vídeo en alta definición era necesario aumentar la capacidad de los soportes. De las dos propuestas, Blu-ray es el formato que se ha mantenido al decidir Toshiba abandonar la fabricación en 2008. Recibe este nombre porque emplea un láser de color azul.

2.2.3.1.3 SSD (En sus siglas en inglés. Solid State Disk)

Una tecnología reciente que cada vez se está expandiendo más rápidamente debido al aumento de la capacidad de los dispositivos que se pueden construir son las comúnmente conocidas como memorias flash y cuyo nombre técnico es el de memoria de estado sólido.

2.2.4 NUBE

Según el sitio acronis.com, “el almacenamiento en nube es un modelo informático para almacenar datos vía internet a través de un proveedor de informática que administra y opera el almacenamiento de la nube como un servicio”.

Existen dos tipos de Nube

2.2.4.1 Pública

Las nubes públicas son la forma más común de implementar esta nueva forma de almacenar datos, las nubes públicas son servidores de proveedores el hardware, software y demás componentes de la infraestructura son propiedad del proveedor de la nube, el almacenamiento de la nube depende de los planes que ofrece el proveedor. Normalmente este tipo de almacenamiento se usan para

proporcionar correos electrónicos web, aplicaciones de Office en línea, almacenamiento y entornos de desarrollo y prueba.

Las ventajas de la nube publica es:

- Costos inferiores.
- No es necesario un mantenimiento.

2.2.4.2 Privada

La nube privada está compuesta por recursos informáticos que utiliza exclusivamente una empresa u organización, esta nube puede estar ubicada dentro de la organización, ya que siempre está conectada a una red privada y el hardware y software se dedican únicamente a la organización. Normalmente esta nube privada suele ser usada por las agencias gubernamentales, instituciones financieras y cualquier organización mediana o grande que realice operaciones esenciales para la empresa. De igual forma la capacidad de almacenamiento es dependiendo de la necesidad del usuario final.

Ventajas:

- La organización puede personalizar el entorno de la nube
- Mejor seguridad

2.2.5 ¿Cuál es la mejor opción?

Para la implementación del sistema de respaldo, es recomendable utilizar el dispositivo de almacenamiento, HDD o Disco Duro en específico los discos duros diseñados para NAS los cuales Western Digital los clasifica por colores, el color asignado para este tipo de discos duros es el RED (Rojo), ya que el modelo RED está diseñado para realizar lectura y escritura de datos por un largo tiempo de

periodo es decir Western Digital lo clasifica como un Disco Duro que puede estar trabajando 24/7.

Como se mencionó, existen muchos tipos de almacenamientos de datos, como el almacenamiento con Cinta Magnética hasta el almacenamiento en la Nube, todos los tipos de almacenamiento funcionan para resguardar información y así ayudar al sistema de respaldo otorgándole un espacio de almacenamiento en el cual respaldará y gestionará la información.

2.3 Causas comunes de pérdida de información

Existen dos causas comunes de pérdida de la información.

Nivel Hardware y Nivel Software.

A nivel Hardware tenemos fallas en los dispositivos de almacenamiento ya sea Disco Duro o SSD.

A nivel Software se puede describir de la misma manera, pero en este caso se enfocará en la falla más común y dañina al mismo tiempo, que sería errores en la actualización del sistema operativo.

2.4 Pérdida de información a nivel hardware

La pérdida de información a nivel hardware depende mucho de la infraestructura que se tenga en las instalaciones donde se resguarda todos los dispositivos que contienen sistemas, páginas web, servidores de correos, servidores de respaldos, etcétera. A esta instalación se le da como nombre SITE.

Actualmente las empresas mexicanas o Arquitectos no toman en cuenta un espacio para el SITE, existen empresas que tienen su SITE en un espacio cerrado y pequeño o ni siquiera contemplan un espacio para instalar un SITE. Estos fallos

son causa común de pérdida de información a nivel Hardware. Ya que el nivel de riesgo y el mal control del SITE conlleva a la pérdida de información.

En estos casos el SITE termina en el piso o en alguna esquina de una oficina, también los equipos de cómputo están instalados en el piso y los usuarios logran patearlos accidentalmente, estos daños físicos causan la pérdida de información a nivel hardware, para esto necesitamos saber que tan grave es la pérdida dependiendo del hardware que utilizamos para almacenamiento.

2.4.1 Disco Duro

Como se sabe el disco duro es el hardware más usado actualmente y por lo tanto sus fallas son las más comunes.

El tiempo de vida del disco duro no es exacto ya que interfiere en muchos factores como, las características del disco duro, el uso del disco duro y las condiciones del disco duro no es posible comparar la vida de un disco duro de una laptop a la vida de un disco duro de un equipo de cómputo o de un equipo de cómputo a la de un servidor.

BACKBLAZE una empresa dedicada al servicio de NUBE, muestra las estadísticas de los discos duros que corren en sus servidores, en el periodo de 2016 a 2019 nos muestran que hay una tasa de fallas del 2.07% en sus discos duros.

Esta tasa de fallas es muy baja teniendo en cuenta de que los discos duros están trabajando desde hace 3 años, pero hay que tener en cuenta los factores que hacen que estos discos duros tengan un periodo de vida tan largo.

Cada disco duro tiene factores que pueden acortar su tiempo de vida o alargarlo.

Los factores que alargan el tiempo de vida de un disco duro son:

- Desfragmentación del disco duro.
- Temperatura baja.

- Libre de Virus informático.
- No tener variaciones de voltaje

Los factores que reducen el tiempo de vida de un disco duro son:

- Variaciones de voltaje.
- Infectado de virus informático
- Temperaturas altas.
- No tiene mantenimiento.
- Daño Físico o Movimientos bruscos.

Estos factores lo que causan en el disco duro es que la información sea ilegible, el formato del disco duro no sea legible o los archivos se dañen y el software no sea capaz de leerlo. En este punto se puede pensar que la información está pérdida y no se puede recuperar, pero una de las ventajas del almacenamiento mecánico es que existen diversos softwares de recuperación de archivos que pueden recuperar la información pérdida y si no da resultado el método mencionado existen laboratorios de recuperación de información.

2.4.2 SSD (Solid-tate drive)

La pérdida de información con el SSD será diferente, recordando que los SSD es un tipo de almacenamiento volátil y su modo de funcionamiento está basado en la tecnología de silicio en la cual el método de almacenar información no es con un disco magnético si no que se sustituye con niveles de voltaje el cual guarda información en las celdas de los chips que tiene integrado el SSD. Por lo tanto, no hay movimiento del hardware como lo realiza un disco duro mecánico así que algún movimiento del equipo no afectará el funcionamiento de este.

Según el sitio Xataka el SSD tiene una duración de lectura y escritura de 72TB entonces si se realiza una lectura u escritura de 40 GB por día, se puede decir que un SSD de 128 GB duraría 5 años.

Xataka habla de un SSD que no tenga factores de riesgo recordando que el SSD funciona con voltaje. El peor factor de riesgo que tendrá el SSD será una variación de voltaje.

Cuando un SSD llega al límite de lectura y escritura empieza a marcar sectores defectuosos, pero aun nos permite realizar un respaldo de la información guardada, pero cuando existe una variación de voltaje y este daña el SSD ya no vuelve a encender y recuperar la información del SSD es imposible.

2.5 Pérdida de información a nivel software

Existen diversos errores para perder información a nivel software, por ejemplo, Software Pirata, trabajar con un software sin licenciamiento, trabajar con diferentes versiones del software por ejemplo que un usuario trabaje con Office 2007 y que otro usuario trabaje con Office 365. Pero el problema más grave de pérdida de software es cuando el Sistema Operativo se actualiza y durante el proceso ocurren catástrofes.

2.5.1 Actualización de Sistema Operativo

La pérdida de información al actualizar el sistema operativo es muy común entre los usuarios ya que el usuario no se da cuenta cuando el sistema operativo pide actualizar, trabajan sus archivos y guardan las modificaciones, al momento de apagar el equipo el sistema operativo actualiza y el usuario al no tener tiempo para esperar a que actualice, en ocasiones fuerza el apago del equipo o en el peor de los casos se va la luz y el equipo de cómputo se apaga mientras se actualizaba el sistema operativo.

Al momento de encender puede suceder dos casos.

En el peor de los casos es que el sistema operativo restaure a un punto anterior ya que los registros de la información guardada durante el último periodo de tiempo van a desaparecer, pueden ser rescatables pero la mayoría de las veces se daña la información.

En el mejor escenario posible es que el sistema operativo deje de funcionar y así se pueda sacar la información directamente del disco duro y mantener la información actualizada.

La forma correcta de solucionar esta pérdida de información es dando mantenimiento al equipo de cómputo, mantener un control de las actualizaciones o desactivarlas, aunque al desactivar las actualizaciones es un grave problema de seguridad porque las actualizaciones parchan fallos de seguridad del sistema y es importante mantener actualizado los parches de seguridad del equipo, es importante realizar campañas para capacitar al usuario y mencionar que espere a que el sistema operativo se actualice por completo, esté conectado a la luz o tenga un no break de respaldo para no interrumpir este proceso.

2.6 Pérdida de información a nivel usuario

En el ámbito laboral la pérdida de información también puede ser causada por el usuario final, ya que la tasa de error es más grande y solamente se preocupan en sacar el trabajo, sin darle la importancia necesaria al resguardo de la información.

Es importante capacitar al usuario, aunque es difícil y no todos los usuarios prestan atención al respaldo de información, este nivel de pérdida es el más común y al que se debe de estar más precavido, por experiencia laboral a continuación se revisara puntos que se consideran de malos hábitos en los usuarios y como solucionar este problema.

2.6.1 Malos Hábitos

Los usuarios finales tienen malos hábitos al laborar e intentan usar el ordenador de una empresa como si fuera un ordenador personal, por ejemplo:

- No guardar los cambios que se realizó en un documento.
- No realizar respaldo periódicamente de la información,
- Forzar el apagado del equipo de cómputo.
- Instalar software pirata.
- Abrir archivos con virus.

Para solucionar estos errores se tiene que llevar un correcto control en el sistema operativo, por ejemplo, metiendo el equipo a dominio y así restringir funciones de administrador al usuario, tener el equipo conectado a un no break, bloquear los puertos USB de los equipos, limitar la navegación en internet, tener el equipo de cómputo dentro de un sistema de respaldos, etcétera. De igual forma la complejidad del error depende mucho de la acción que realizo el usuario final ya que en algunas ocasiones el daño también es físico.

2.7 Importancia del almacenamiento

Después de conocer los tipos de almacenamiento y las causas comunes de pérdida de información, es importante tener en cuenta que es lo que estamos almacenando y la importancia que tiene almacenar la información que tenemos asignada, no es lo mismo guardar información de una organización al resguardo de información personal. Para esto debemos de conocer la importancia del almacenamiento de estas.

2.7.1 Importancia del almacenamiento en una Organización

Cuando se habla de información en la organización se hace referencia a datos que son esenciales para el proceso diario de una organización, es importante saber que está información es vital para una empresa ya que si llega a existir una pérdida de información y no se cuenta con ningún método viable de recuperación, entonces se está hablando de meses de retraso de operación y pérdida de dinero, por lo tanto es de suma importancia respaldar la información de una organización cualquier dato es vital en algún momento.

Cuando un empleado renuncia o es dado de baja en una organización normalmente, tanto el usuario final o el personal de sistemas, elimina la información del usuario para tener más almacenamiento en el equipo usado, este procedimiento es erróneo y por ningún motivo se debe de pensar en eliminar información dentro de una organización, en estos casos se debe de almacenar la misma del usuario para futuras consultas.

Si se tiene la información operativa de la empresa, datos de los trabajadores y respaldo de ambos, es importante tener una buena estructura para el correcto control de respaldo de ésta.

2.7.2 Importancia del almacenamiento Personal

Normalmente se hace referencia a videos, fotos, música, archivos de trabajo, pero a lo que no se da importancia hoy en día, con el fin de realizar trámites personales o incluso una contratación laboral, se escanean las identificaciones emitidas por el Instituto Nacional Electoral (INE), se escanea recibos de agua, luz, gas, etcétera. Esta información personal es objetivo para un hacker ya que lo que ellos buscan son bases de datos de datos con información personal, dentro de páginas web, sistemas públicos o sistemas de las organizaciones por lo cual es vital tener una infraestructura correcta para el resguardo de este tipo de información.

Capítulo 3. Red informática

3.1 ¿Qué es una red informática?

Según Andrew s. Tanenbaum y David J. Wetherall, en su libro de Redes de Computadoras una red es “una colección de computadoras interconectadas mediante una sola tecnología”.

De igual forma los autores Armando Moisés Bernal Kaiser y Mireya López Escobar, nos mencionan en los Apuntes Digitales 2012 de la Universidad Nacional Autónoma de México Facultad de la Contaduría y Administración, que las redes son una “Interconexión entre computadora y equipo de computación de un edificio, país o el mundo para hacer posibles la comunicación electrónica.”

Se puede definir que una red es un grupo de computadoras interconectadas mediante una tecnología con el fin de obtener una comunicación electrónica.

3.2 Estructura de la red informática

La redes o red informática tienen dos niveles de componentes: Hardware de red, Software de Red.

Andrews Tanenbaum y David J. Wetherall en ambos niveles mencionan detalladamente de cómo se conforman estos niveles de componentes. En el nivel de Hardware y Software, mencionando los tipos de red (LAN, MAN Y WAN).

En la Universidad Nacional Experimental Simón Rodríguez de Venezuela, el Profesor Palo Verde, en su curso de procesamiento de datos, explica de una forma sencilla la estructura de las redes.

El software de las aplicaciones: son aquellos programas que se comunican con los usuarios de la red y permiten compartir información (como los archivos, gráficos o vídeos) y recursos (como impresoras o unidades de disco).

El software de red: son los programas que establecen protocolos para que los ordenadores se comuniquen entre sí, los cuales envían y reciben grupos de datos formateados denominado paquete.

El hardware de red: formado por los componentes materiales que unen los ordenadores.

Dos componentes importantes son los medios de transmisión que transportan las señales de los ordenadores (cables o fibras ópticas) y el adaptador de red, que permite acceder al medio material que conecta a los ordenadores, recibir paquetes desde el software de red y transmitir instrucciones y peticiones a otros ordenadores.

Entonces en una estructura de red Informática es necesario tener un emisor y un receptor, pero de igual forma es necesario tener aplicaciones para la comunicación de usuario a usuario por medio de la red y el software para establecer los protocolos que se utilizarán para que los ordenadores estén comunicados entre sí y así puedan ser capaces de enviar y recibir paquetes

3.3 Tipos de Redes

Existen diferentes tipos de redes dependiendo de su uso se le asigna un tipo de red ya que no podemos decir que una red de hogar es lo mismo que la red de una cuidad.

En un post de la Universidad de Valencia explica las similitudes y diferencias entre las principales redes utilizadas para conectar ordenadores y dispositivos.

3.3.1 LAN (Local Area Network)

Local Area Network. Las Redes de Área Local son las más utilizadas en el intercambio de datos y recursos entre ordenadores. Habitualmente se utilizan para

conectar equipos en espacios relativamente pequeños. Su principal característica es que permiten la interconexión de múltiples nodos (unidades de almacenamiento, impresoras y otros dispositivos) aunque no estén conectados físicamente a nuestros ordenadores. El principal inconveniente es que los nodos que se pueden conectar a una LAN son limitados.

Este tipo de red es el que se encuentra en todos lados, ya que cada oficina o casa es una red LAN, recordando que una red LAN es limitada, todos los lugares con usuarios pequeños se trabaja una red LAN para mantenerlos comunicados entre ellos.

3.3.2 WAN (Wide Área Network)

Citando nuevamente la Universidad de Valencia, Wide Area Network. Cuando varias redes LAN se conectan entre ellas se las conoce por el nombre de Redes de Área Amplia. Las conexiones WAN más comunes son la línea telefónica y los satélites. Las grandes compañías y los proveedores de servicio de Internet (ISP, por sus siglas en inglés) utilizan frecuentemente este tipo de redes.

3.3.3 MAN (Metropolitan Area Network)

Metropolitan Area Network. En cuanto a la cobertura geográfica, las Redes de Área Metropolitana tienen mayor alcance que las LAN, pero menos que las WAN, por eso se emplean principalmente en ámbitos más reducidos como ciudades y pueblos. El principal medio conductor que se emplea en la transferencia de información es la fibra óptica, lo que permite no solo una conexión más rápida, sino también tasas de errores y latencia (la suma de retardos temporales de una red) más bajas que otras redes. Además, también son más estables y resistentes a las interferencias radioeléctricas.

3.3.4 WLAN (Wireless Local Network)

Wireless Local Network. A diferencia de las Redes de Área Local o LAN, en las redes de Área Local Inalámbricas el intercambio de información se realiza a través de ondas de radio. El principal inconveniente es la inseguridad: cualquier persona con una terminal inalámbrica puede conectarse a otro punto de acceso privado si este carece de las medidas de seguridad apropiadas.

3.3.5 WMAN (Wireless Metropolitan Network)

Wireless Metropolitan Network. La Red Metropolitana Inalámbrica es la versión inalámbrica de las Redes de Área Metropolitana convencionales. La principal diferencia con las MAN es que su alcance es mucho mayor. Esta tecnología está presente en estándares de comunicación como el WiMAX (Interoperabilidad Mundial para Acceso con Microondas, por sus siglas en inglés).

3.3.6 WLAN (Wireless Local Area Network)

Wireless Local Area Network. La Red Inalámbrica de Área Amplia tiene una cobertura geográfica mucho más amplia que la que ofrecen las redes WMAN. En vez de usar tecnologías de comunicaciones móviles como WiMAX, UMTS, GPRS, EDGE, CDMA2000, GSM, CDPD, Mobitex, HSPA y 3G; utiliza sistemas como el wifi y el LMDS (Sistema de Distribución Local Multipunto, por sus siglas en inglés).

3.3.7 SAN (Storage Area Network)

Storage Area Network. La Red de Área de Almacenamiento es un tipo de red muy utilizada por las empresas de mayor tamaño porque permite conectar varias

unidades de almacenamiento a las Redes de Área Local o LAN. Este tipo de redes se utilizan en los ordenadores centrales encargados de procesar gran cantidad de datos de compañías como IBM, SUN y HP.

3.3.8 PAN (Personal Area Network)

Personal Area Network. La Red de Área personal conecta los dispositivos cercanos al usuario en un entorno reducido. Ordenadores, puntos de acceso a Internet, teléfonos móviles, PDA e impresoras se pueden conectar a una red PAN.

3.4 Topología de red

El autor Salvador Meza Badillo especializado en informática de la Facultad de Contaduría y Administración de la Universidad Nacional Autónoma de México menciona que la topología de red puede ser física y lógica.

Física: se describe como el cable que conecta a los nodos.

Lógica: refiere a la forma en que la información fluye a través de la red.

Se puede definir que la topología de red es el método que se utilizará dentro de una infraestructura de red, para evitar conflicto de envío y recepción de datos.

Es muy importante que antes de elegir la topología de la red, es necesario tener en cuenta la importancia de la infraestructura que se tiene implementada o se va a implementar, por experiencia, es recomendable tener en cuenta los siguientes puntos:

- Cantidad de computadoras
- Tipo de computadoras
- Aplicación de voz, video y datos
- Tipo de red

- Transmisión de datos vía inalámbrico o cableado
- Tipo de conectores
- Adaptadores de red

Una vez que se tengan estos puntos claros y definidos, es sencillo definir la topología, citando de nuevo al autor Salvador Meza Badillo, menciona a continuación las siguientes topologías.

3.4.1 Bus

Utiliza un único segmento backbone (longitud del cable) al que todos los hosts se conectan de forma directa, si un nodo falla, la red continuaría funcionando, pero si se presenta un problema en el bus, todo el sistema deja de trabajar.

3.4.2 Estrella

En esta configuración todos los nodos terminales están conectados a un elemento central que generalmente es un concentrador o switch, si uno de los nodos terminales falla no afecta a los demás, si el elemento central presenta problemas, la red completa dejara de funcionar.

3.4.3 Anillo

Esta topología conecta un host con el siguiente y el ultimo host con el primero creando un anillo físico. Esto es que todos los nodos están conectados el uno con el otro, formando una cadena o círculo cerrado. En algunas implantaciones cada nodo trabaja como un repetidos activo, cuando un nodo falla, la continuidad del anillo se interrumpe y todo el sistema se paraliza, en la implantación pasiva, existen elementos adicionales que garantizan una tolerancia a gallas de los nodos.

3.4.4 Malla

Cada host tiene sus propias conexiones con el demás host (múltiples rutas hacia cualquier lugar), topología de alta redundancia. Es una configuración de malla, la existencia de múltiples rutas físicas de comunicación entre dos nodos garantiza una alta disponibilidad. En una configuración de malla completa, cada nodo de la red requiere al menos un enlace con cada uno de los otros nodos. Conforme el número de nodos aumenta la cantidad de enlaces necesarios también crece, pero geométricamente, esto eleva considerablemente los costos y no siempre garantiza un uso eficiente de cada enlace.

3.4.5 Estrella extendida

Enlaza estrellas individuales conectando los dispositivos, esto permite extender la longitud y el tamaño de la red.

3.4.6 Jerárquica

Similar a la estrella extendida, solo que conecta a una computadora (servidor) que controla el tráfico.

3.5 Protocolo de redes

Según EcuRed, Los protocolos son reglas de comunicación que permiten el flujo de información entre equipos que manejan lenguajes distintos, por ejemplo, dos computadores conectados en la misma red, pero con protocolos diferentes no podrían comunicarse jamás, para ello, es necesario que ambas "hablen" el mismo idioma.

Por lo tanto, no existe un solo protocolo de red ya que un ordenador puede pertenecer a diferentes redes y cada red tenga un protocolo para estar comunicados. No es necesario saber todos los protocolos, pero si conocer los más utilizados según EcuRed.

3.5.1 FTP (File Transfer Protocol)

Protocolo de Transferencia de Archivos. Proporciona una Interfaz y servicios para la transferencia de archivos en la red.

3.5.2 SMTP (Simple Mail Transfer Protocol)

Protocolo Simple de Transferencia de Correo. Proporciona servicios de correo electrónico en las redes Internet e IP.

3.5.3 TCP (Transmission Control Protocol)

Protocolo de Control de Transporte. Es un protocolo de transporte orientado a la conexión. TCP gestiona la conexión entre las computadoras emisora y receptora de forma parecida al desarrollo de las llamadas telefónicas.

3.5.4 UDP (User Datagram Protocol)

Protocolo de Datagrama de Usuario. Es un protocolo de transporte sin conexión que proporciona servicios en colaboración con TCP.

3.5.5 IP (IP address)

Protocolo de Internet. Es la base para todo el direccionamiento que se produce en las redes TCP/IP y proporciona un protocolo orientado a la capa de red sin conexión.

3.5.6 ARP (The Address Resolution Protocol)

Protocolo de Resolución de Direcciones. Hace corresponder las direcciones IP con las Direcciones MAC de hardware.

3.6 La red informática y la información

Es importante saber cómo se relaciona la red y la información antes de entrar al mundo de respaldos, a pesar de que a lo largo del trabajo se explicó que es la información y que es la red, es el momento de saber cómo funciona al momento de juntarlos.

3.6.1 ¿Cómo se relacionan?

La información es el material principal para el conocimiento, los datos, investigaciones, reportes, etcétera. Las redes informáticas nos otorgan espacios virtuales, envío y recepción de datos a nivel mundial, con tal de mantener actualizados en información a empresarios, usuarios, etcétera.

Al unir las redes informáticas y la información, se genera o se crea una red de información el cual permite estar en constante comunicación. Con esta red de información se puede enviar la información vía protocolo SMB o se puede compartir la información vía el protocolo FTP, sin importar que sea una red pública o privada,

los equipos o usuarios están en constante comunicación y son capaces de visualizar la información en cualquier parte del mundo siempre y cuando tengan la conexión directa hacia los servidores de su empresa.

3.6.2 Servidor de información

Existen diferentes tipos de servidor. Servidor web, este puede almacenar páginas web dentro de y así para que nosotros podamos visualizarlas e interactuar con ellas. Servidor de correo, este se encarga de gestionar él envió y la recepción de correos etcétera. El servidor que se necesita para este caso es un servidor de información el cual solamente se dedica a resguardar información y compartir la misma.

Estos servidores se les conoce comercialmente como NAS.

3.6.3 NAS (Network-attached storage)

Según Seagate, empresa dedicada a la creación de dispositivos de almacenamiento, “un sistema NAS es un dispositivo de almacenamiento conectado a una red que permite almacenar y recuperar datos en un punto centralizado para usuarios autorizados de la red y multiplicidad de clientes. Los dispositivos NAS son flexibles y expansibles; esto lo que implica es que a medida que vaya necesitando más capacidad de almacenamiento, podrá añadirla a lo que ya tiene. Un dispositivo NAS es como tener una nube privada en la oficina. Es más veloz, menos costoso y brinda todos los beneficios de una nube pública dentro de los predios, lo cual le da a usted todo el control”.

El sistema NAS utiliza Discos Duros Mecánicos como método de almacenamiento, los NAS es la opción más correcta para almacenar información ya que permiten acceso a los datos de las empresas las 24 horas.

El almacenamiento de este sistema es variado ya que depende del modelo que se adquiera, existen NAS que soportan 16 TB hasta 144 TB, el almacenamiento del NAS es muy accesible ya que se asigna conforme las necesidades del usuario final.

Con un sistema NAS, la información siempre está accesible, lo cual facilita la operación de los usuarios, responder a clientes en tiempo y forma, así como dar seguimiento inmediato a otros asuntos. Se puede decir que un NAS es una nube privada en el cual como usuario final puede tomar el control de la información y decidir quién tiene acceso a la información y quién no.

3.7 La nube y la información

Antes que nada, se debe de conocer ¿qué es la nube?

Según Microsoft Azure la nube es “una red mundial de servidores, cada uno con una función única. La nube no es una entidad física, sino una red enorme de servidores remotos de todo el mundo que están conectados para funcionar como un único ecosistema.”

Existen diferentes tipos de servicios que otorga la nube hoy en día, pero en este caso se necesita el servicio de “Almacenamiento en nube” el cual Según AWS (Amazon Web Services) dice que “El almacenamiento en la nube se compra a un proveedor de la nube externo que posee y opera capacidad de almacenamiento de datos y la distribuye a través de Internet con un modelo de pago por uso. Estos proveedores de almacenamiento en la nube administran la capacidad, la seguridad y la durabilidad para lograr que sus aplicaciones de todo el mundo tengan acceso a los datos.”

3.7.1 ¿Cómo se relacionan?

El servicio de almacenamiento de nube y la cantidad de información que se quiere transmitir día a día entre usuario y cliente es la mejor combinación que puede existir, ya que la nube permite acceder a su interfaz desde cualquier dispositivo sin necesidad de estar dentro de un protocolo estricto como es requerido en una red informática, solamente es necesario tener un cliente descargado y las credenciales para acceder al almacenamiento privado o público que otorga la nube, por lo tanto el acceso a la información vía nube es demasiado sencillo y práctico en el ámbito empresarial ya que no hay necesidad de realizar ninguna configuración y solamente el usuario final se dedicaría a alimentar el almacenamiento de la nube con la información solicitada.

3.7.2 Servicios

La nube ha crecido tanto, que día a día crean nuevos servicios, por ejemplo, AWS ofrece servicios de nube desde una base de datos hasta servidores que corren código en la nube. No es necesario conocer todos los servicios de la nube, pero si hay que conocer lo que se necesita al momento de resguardar nuestros datos o información y para esto es el servicio de Almacenamiento en la Nube.

El servicio de almacenamiento en la nube, son servidores dedicados a almacenar información en este caso NAS, al utilizar estos servidores se deben de tomar dos aspectos en cuenta a la hora de rentarlos, Almacenamiento y Periodo, pero si se llega a contratar el servicio en la nube no se rentará un servidor completo, en estos casos se podrá rentar una pequeña parte del servidor y su almacenamiento.

Viendo los precios que Acronis, empresa dedicada a respaldos de la información, se puede ver que ofrece los siguientes precios:

Almacenamiento	Periodo de licencia	Precio final / por mes
250 GB	1 AÑO	$299.00
500 GB	2 AÑO	$499.00
1 TB	3 AÑO	$899.00
2 TB	4 AÑO	$1,749.00
3 TB	5 AÑO	$2,649.00
4 TB	6 AÑO	$3,499.00
5 TB	7 AÑO	$4,299.00

Tabla Núm. 1 Precios Acronis 3.2 (en dólares) Fuente: acronis.com

De igual forma AWS presenta lista de precios, pero toma en cuenta características diferentes que Acronis, ya que AWS en vez de cobrar por almacenamiento cobra por Gigabyte, según su página de precios si se almacena 50 TB por mes, AWS estará cobrando 0,23 USD por cada Gigabyte y teniendo en cuenta que 1 TB contiene 1,000 Gigabyte, es decir un precio final de 11,500.00 dólares por mes.

3.8 ¿Cuál es la mejor opción para almacenar información?

Para elegir la mejor opción hay que tener uno o varios factores a la hora de implementar en una empresa o en nuestra empresa, los cuales serían: Inversión, Infraestructura, Usuarios, etcétera.

En resumen las opciones de las distintas formas de almacenar la información previamente mencionadas, podemos decir que para implementar un almacenamiento vía local es necesario de una gran inversión en la infraestructura informática de la empresa tomando en cuenta tener personal altamente capacitado para que lleve el control de la información y el mantenimiento de la misma, de la misma manera si rentamos los servidores en la nube el almacenamiento de la información es más sencillo ya que no se invertirá en NAS y solamente en personal altamente capacitado para darle mantenimiento a los NAS y gestionar el sistema

de respaldo, pero la renta de servicio en nube no es nada barata y el control de la información no la tendríamos totalmente ya que seriamos dispensables de la infraestructura que el proveedor ofrece.

Capítulo 4. Seguridad informática

Es importante saber que la seguridad informática es de vital importancia conocerla, es la que se encarga de la información que se transmita o se tenga respaldada sea correcta (integridad), también se encarga de toda la información personal no sea divulgada a personas o sistemas informáticos (confidencialidad) y se encarga de que toda información sea accesible cuando se necesite (disponibilidad), dado que existen usuarios que buscan o roban la información con el fin hacer mal uso de esta, es necesario conocer de la seguridad informática.

4.1 ¿Qué es la seguridad informática?

La Universidad de Valencia España, nos menciona que la seguridad informática es:

“El proceso de prevenir y detectar el uso no autorizado de un sistema informático”.

Según Cisco menciona que:

Es el conjunto de políticas, procesos y herramientas de hardware y software, que se encargan de proteger la privacidad, la disponibilidad y la integridad de la información y los sistemas en una red.”

Sin embargo, se puede concluir que la seguridad informática, es el conjunto de políticas, herramientas de hardware y software las cuales se encargan de proteger la disponibilidad, integridad y viabilidad de los sistemas informáticos.

4.2 Ataques informáticos

Según el sitio ecu red, un ataque informático “Es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un sistema informático o red.”

Los ataques informáticos para el robo de información son por medio de Ransomware, Spyware y Phishing.

4.2.1 Ransomware

Según Malwarebytes, empresa especializada anti-malware menciona que el Ransomware es un *es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de Ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal. Hoy en día los creadores de Ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito.*

4.2.1.1 ¿Cómo se puede infectar el equipo de cómputo?

El Ransomware puede infectar de varias maneras, uno de los métodos más habituales dentro del mundo empresarial es enviando spam malicioso, este spam se envían por medio de mensajes o correos maliciosos los cuales incluyen archivos adjuntos o sitios web como trampa, por ejemplo, un Ransomware puede contener PDF que se hagan pasar por reportes empresariales, al momento de abrir este archivo, automáticamente el malware accede al sistema y empieza a bloquear el sistema operativo.

4.2.1.2 Tipos de Ransomware

Existen diferentes tipos de Ransomware, cada uno afecta la información guardada en el equipo de cómputo, ya que ese es el objetivo del virus, siempre atacara la información que se tiene almacenada, pero siempre ataca de diferente forma y para esto se clasificaron dependiendo de la gravedad de la situación.

Es importante conocer a cada tipo de secuestro de información para saber cómo reaccionar ante dicha situación y así poder lograr la recuperación total de la información.

4.2.1.2.1 Bloqueadores de pantalla

Citando de nuevo a Malwarebytes, *Si un Ransomware que bloquea la pantalla llega a su ordenador, le impedirá el uso de su PC por completo. Al encender el ordenador aparece una ventana que ocupa toda la pantalla, a menudo acompañada de un emblema de aspecto oficial del FBI o del Departamento de Justicia de los Estados Unidos, que le indica que se han detectado actividades ilegales en su ordenador y que debe pagar una multa. Sin embargo, el FBI no actuaría nunca así ni le exigiría ningún pago por la realización de una actividad ilegal. En caso de que sospecharan que usted comete piratería, o que está en posesión de pornografía infantil o por cualquier otro delito informático, el FBI seguiría los canales legales adecuados.*

4.2.1.2.2 Ransomware de cifrado

Este es el peor de todos. Este es el que le secuestra los archivos y los cifra, exigiendo un pago para volver a descifrarlos y devolvérselos. La razón por la que este tipo de Ransomware es tan peligroso es porque una vez que los ciberdelincuentes se apoderan de los archivos, no hay ningún software de seguridad

ni restauración del sistema capaz de devolvérselos. A menos que pague el rescate, puede despedirse de sus archivos. E incluso si lo paga, no hay ninguna garantía de que los ciberdelincuentes le devuelvan los archivos.

4.2.1.3 ¿Como protegerse de la infección?

Los Ransomware normalmente abundan en el internet o en software pirata, entonces para llevar un correcto control de este peligro para la información, se debe de tomar en cuenta los siguientes puntos para prevenir un ataque de Ransomware.

- Controlar el tráfico de red.
- Limitar los valores de navegación en internet
- Detectar y controlar el spam de correo.
- Realizar una blacklist de los correos de spam.
- No utilizar software pirata.

4.2.1.4 ¿Qué hacer en caso de infección?

En caso de no tener un respaldo del equipo dañado, se necesita restaurar el sistema operativo a un punto anterior del suceso, si no se puede restaurar el sistema a un punto anterior, lo recomendado es realizar una partición del disco duro o conectar el disco duro afectado a una maquina con un sistema previamente cargado y adquirir desencriptadores gratuitos o adquirir uno de paga y empezar con el proceso de desencriptar la información y así volver la a recuperar la información.

4.2.2 Spyware

El objetivo del spyware comparado al de Ransomware es el mismo, pero con diferente tipo de información, lo que realiza el spyware es recopilar información

personal en tiempo real, ya sean usuarios y contraseñas de sitios web y tarjetas de crédito.

Según MalwareBytes un Spyware *es un software malicioso que infecta su ordenador o dispositivo móvil y recopila información sobre usted, su navegación y su uso habitual de Internet, así como otros datos*.

4.2.2.1 ¿Cómo puede infectar a mi equipo?

El spyware puede infectar el equipo de igual forma que el malware, mediante un troyano, un virus, un gusano, un exploit u otro tipo de malware, pero para detectar un intento de ataque es necesario tener en cuenta las técnicas empleadas por el spyware.

Para esto malwarebytes nos enlista las técnicas más usadas por el spyware:

- ***Vulnerabilidades**. No haga clic bajo ningún concepto en un enlace desconocido o en un archivo sospechoso que se haya adjuntado a un correo electrónico y que abra un archivo ejecutable o acceda a un programa en línea que descargue e inicie («ejecute») una aplicación.*
- ***Marketing engañoso**. Los creadores de spyware tienen como estrategia presentar sus programas de spyware como herramientas de gran utilidad que conviene descargar. Puede ser un acelerador de Internet, un nuevo gestor de descargas, un programa de limpieza de disco duro o un buscador web alternativo.*
- ***Paquetes de software**. ¿A quién no le gusta el software gratuito (software libre o freeware)? La única excepción: cuando se trata de un programa host que oculta un complemento, extensión o plugin malicioso. Lo que a simple vista parece un componente necesario puede ser en realidad spyware, que se mantiene activo a pesar de haber desinstalado la aplicación que lo ocultaba.*

- ***Spyware de dispositivos móviles**. El spyware móvil existe desde que se generalizó el uso de dispositivos móviles. Dado que los dispositivos móviles son pequeños y los usuarios no pueden ver todo lo que se está ejecutando, es posible que estas acciones se desarrollen de forma inadvertida en segundo plano. La instalación de una aplicación con código malicioso provoca la infección de los dispositivos Mac y Android. Entre estos programas se incluyen aplicaciones auténticas con código malicioso, aplicaciones maliciosas con nombre falso y aplicaciones con enlaces de descarga falsos.*

Estas precauciones se pueden implementar mediante una restricción de navegación, pero en caso de que no se tenga la infraestructura para realizar dicha restricción, hay que tomar en cuenta las técnicas que utilizan los creadores del spyware para capacitar a los usuarios y así mantener una cultura informática.

4.2.2.2 Tipos de Spyware.

Igual que el Ransomware, el spyware tiene diferentes tipos de amenazas, aunque tienen el mismo objetivo unos spyware se especializan en una sola información.

Malwarebytes ayuda con el recolectado de los tipos de Spyware que se especializan en una sola información.

4.2.2.2.1 Ladrones de contraseñas

Son aplicaciones diseñadas para hacerse con las contraseñas de los ordenadores infectados. Entre los tipos de contraseñas recopiladas se incluyen credenciales almacenadas de navegadores web, credenciales de inicio de sesión y diversas contraseñas personales.

4.2.2.2.2 Troyanos bancarios

Son aplicaciones diseñadas para conseguir las credenciales de instituciones financieras. Aprovechan las vulnerabilidades que presenta la seguridad del navegador para modificar páginas web, alterar el contenido de transacciones o añadir transacciones adicionales, de manera totalmente encubierta e invisible tanto para el usuario como para la aplicación host.

Los troyanos bancarios pueden afectar a una gran variedad de instituciones financieras, entre ellas los bancos, portales y carteras digitales, de igual forma recaudan información aprovechando la vulnerabilidad del ataque, resguardando esta información en servidores remotos para la recuperación de ésta.

4.2.2.2.3 Infostealers

Son aplicaciones capaces de analizar un ordenador infectado y buscar distintos tipos de datos, como nombres de usuarios, contraseñas, direcciones de correo electrónico, historiales de navegación, archivos, información del sistema, documentos, hojas de cálculo o archivos multimedia.

Al igual que los troyanos bancarios, los infestarles se aprovechan de las vulnerabilidades de seguridad del navegador para recopilar información de usuarios y contraseñas.

4.2.2.2.3 Keyloggers

También conocidos como registradores de pulsaciones de teclas, son aplicaciones diseñadas para capturar la actividad del ordenador, es decir, para registrar las pulsaciones de teclas, las visitas a sitios web, el historial de búsquedas, las conversaciones por correo electrónico, las participaciones en chats y las

credenciales del sistema. Por lo general, recopilan capturas de la ventana actual con una frecuencia programada. Los registradores de pulsaciones de teclas también desarrollan funciones que permiten capturar y transmitir imágenes y archivos de audio o vídeo de forma clandestina desde cualquier dispositivo conectado. Asimismo, pueden permitir a los atacantes recopilar documentos impresos en impresoras conectadas, que pueden transmitirse después a un servidor remoto o almacenarse localmente para su posterior recuperación.

Este spyware es el más peligroso ya que como menciona malwarebytes recauda cualquier pulsación que realicemos en el teclado, tomando en cuenta que el keylogger tiene la capacidad de tomarnos fotos por medio de una webcam que tengamos conectada en nuestro equipo, también puede grabar sonido mediante los micrófonos que se encuentren conectados al ordenador. Estas aplicaciones normalmente es necesario instalarlas ya que no se pueden ejecutar como un malware, una vez instalada el keylogger reportará por medio de correos o reportes guardados en un servidor remoto y así mantener informado al creador del keylogger.

4.2.2.3 Qué hacer si hay infección

Normalmente, este tipo de virus no levanta sospecha alguna, lo cual lo hace más complicado de detectar, pero no es imposible, hay que tener en cuenta los siguientes puntos para saber si tenemos un spyware instalado en el ordenador.

Mal rendimiento del equipo

Normalmente los spyware no levantan sospecha alguna, pero hay ocasiones donde los usuarios notan un rendimiento más lento de lo habitual y es cuando se dan cuenta que el procesador o disco duro está trabajando al 100% nada más al

momento de encender el ordenador y no realizar ninguna tarea dentro del equipo, es importante notar este tipo de rendimiento para realizar un análisis con el antivirus.

Inicios de sesión no autorizados

Es importante tener las cuentas personales ligadas al número de teléfono, así tendrán la opción de verificación de dos pasos y el mismo portal notificará cuando alguien intenta iniciar sesión, notando esto es importante realizar un cambio de contraseñas y un análisis al ordenador donde se labora.

Activación no autorizada de micrófono y webcam

Es notable cuando la webcam y el micrófono funcionan sin autorización previa, ya que al momento de estar funcionando el led de notificación del dispositivo se enciende, al detectar este comportamiento es necesario realizar un análisis en nuestro equipo o normalmente lo que los usuarios realizan para no tener este problema es tapar con una cinta la webcam y el micrófono del ordenador.

4.2.2.4 Como protegerse de la infección

Malwarebyte nos enlista unas medidas básicas de defensa contra los spyware.

- *No abra correos electrónicos de remitentes desconocidos.*
- *No descargue archivos a menos que provengan de una fuente fiable.*
- *Coloque el ratón sobre los enlaces antes de abrirlos y asegúrese de acceder a la página web correcta.*

Sin embargo, como los usuarios han mejorado su conocimiento sobre la protección contra este tipo de amenazas, los hackers han desarrollado métodos más sofisticados para la transmisión del spyware, para ello se recomienda la instalación de un buen antivirus o antimalware, capaz de realizar un análisis en tiempo real para hacer frente a las nuevas formas de spyware avanzado y así detectarlas justo a tiempo antes de que recolecten alguna información valiosa del equipo infectado.

4.2.3 Phishing

Según malwarebytes el phishing es *el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o "suplanta su identidad") a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.*

Si un usuario pica el anzuelo y hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña. Si es lo suficientemente ingenuo y lo hace, la información de inicio de sesión llega al atacante, que la utiliza para robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro.

Entonces se puede concluir que el Phishing o también conocido como ingeniería social, es la forma de engañar a los usuarios para que compartan

información confidencial, ya sean contraseñas, números de tarjeta de crédito, etcétera. A través de correos que suplantan la identidad de un usuario real u organización y así el usuario ingresa información conscientemente para que esa información se guarde en un servidor remoto y así el responsable del phishing tenga la información en sus manos.

4.2.3.1 Tipos de ataques de phishing

Existen dos tipos de phishing, para la obtención de información, Spear y Clonación. Es necesario conocer estos dos tipos de phishing ya que en estos casos se debe de saber cómo piensa el atacante a la hora de aplicar este método.

4.2.3.1.1 Spear phishing

Según malwarebytes la mayoría de las campañas de phishing envían correos electrónicos masivos al mayor número posible de personas, el spear phishing es un ataque dirigido. spear phishing ataca a una persona u organización específica, a menudo con contenido personalizado para la víctima o víctimas. Requiere un reconocimiento previo al ataque para descubrir nombres, cargos, direcciones de correo electrónico y similares. Los hackers buscan en Internet para relacionar esta información con lo que han averiguado sobre los colegas profesionales del objetivo, junto con los nombres y las relaciones profesionales de los empleados clave en sus organizaciones. Con esto, el autor del phishing crea un correo electrónico creíble.

El spear phishing es una amenaza critica para las empresas, ya que se realiza un estudio a la víctima que se le enviara el correo malicioso, como se menciona, se realiza una investigación previa para conocer su nombre, cargo, direcciones, correo electrónico, amistades, etcétera. Cualquier información adicional de la víctima es importante ya que, con base en lo anterior, el correo se

crea y se envía, se puede hacer pasar como el proveedor de la empresa, director o hasta en un familiar.

Con estos engaños se pide información personal o hasta transacciones bancarias.

4.2.3.1.1 Phishing de clonación

Según malwarebytes *el phishing de clonación, los delincuentes hacen una copia, o clonan, correos electrónicos legítimos enviados anteriormente que contienen un enlace o un archivo adjunto. Luego, el autor del phishing sustituye los enlaces o archivos adjuntos con contenido malicioso disfrazado para hacerse pasar por el auténtico. Los usuarios desprevenidos hacen clic en el enlace o abren el adjunto, lo que a menudo permite tomar el control de sus sistemas. Luego el autor del phishing puede falsificar la identidad de la víctima para hacerse pasar por un remitente de confianza ante otras víctimas de la misma organización.*

En el peor de los casos, el phishing de clonación, además de clonar un correo electrónico y la identidad del remitente, en el momento de abrir el archivo malicioso puede realizar un spam del correo y reenviar éste con el correo original del remitente y así propagar el virus en todas las cuentas que logren abrir el archivo malicioso. Dado que es fácil de detectar este tipo de ataques pero, de igual forma, si el usuario no se encuentra capacitado, puede causar muchos problemas en las bandejas de entrada de las cuentas de correo.

4.2.3.2 Cómo identificar un ataque de phishing

Reconocer un intento de phishing no es sencillo para las personas que desconocen de este tipo de ataques, es importante que si el correo recibido despierta alguna sospecha del contenido es importante confiar en la intuición ya que

como lo decimos en lo anterior los ataques de phishing son tentadores porque te envían ofertas demasiadas buenas por ejemplo “da clic en el siguiente enlace y te realizamos un 50% de descuento en la próxima compra de tu auto” y este mensaje viene de nissan@free.org, lo que debemos de averiguar es que el correo de Nissan obviamente no puede tener el dominio free.org ya que por ser una empresa de alto nivel es ilógico que sus correo no terminen en @nissan.com. Estos pequeños detalles son los que se deben de tener en cuenta.

Aquí tenemos algunas señales de un intento de phishing.

- El correo electrónico realiza una oferta demasiada buena.
- El mensaje suena aterrador, este tipo de mensaje tiene el objetivo de tener un contenido alarmista, para crear un sentido de urgencia incitando al usuario que haga clic y actúe al momento. Hay que tener en cuenta que las organizaciones no solicitan detalles personales a través de internet.
- El mensaje contiene archivos extraños, estos adjuntos pueden contener malware, Ransomware o alguna otra amenaza online por lo tanto es importante antes de abrir un archivo de procedencia dudosa, analizarlo con el antivirus que este instalado.
- El contenido de correo contiene enlaces un poco extraños, por ejemplo si Apple te envía un correo en donde necesita actualizar los datos de tu cuenta de iCloud y te envían un correo con un botón que dice “da clic aquí” en vez de dar clic podemos asegurarnos en pasar el cursos por encima del enlace para ver la URL (Localizador Uniforme de Recursos) real, se puede ver claramente que la URL que nos envían no tienen nada que ver con la que trabaja Apple, una recomendación es ser útil con las faltas de ortografía ya que son lo que realizan los hacker para falsificar una URL por ejemplo apple.com la URL falsa seria aple.com.

4.2.3.3 Cómo protegerse del phishing

La primera línea de defensa contra el phishing es el criterio de uno mismo, los navegadores, el antivirus si pueden ayudarnos contra esta amenaza, pero el criterio o el conocimiento sobre el tema del usuario es vital para que no se caiga en este tipo de ataque.

Adam Kujawa director de malwarebytes propone algunas prácticas más importantes para mantenerse a salvo de este tipo de ataque.

- *No abra correos electrónicos de remitentes que no le sean familiares.*
- *No haga clic en un enlace dentro de un correo electrónico a menos que sepa exactamente a dónde le lleva.*
- *Para aplicar esa capa de protección, si recibe un correo electrónico de una fuente de que la que no está seguro, navegue manualmente hasta el enlace proporcionado escribiendo la dirección legítima del sitio web en su navegador.*
- *Busque el certificado digital del sitio web.*
- *Si se le pide que proporcione información confidencial, compruebe que la URL de la página comienza con "HTTPS" en lugar de simplemente "HTTP". La "S" significa "seguro". No es una garantía de que un sitio sea legítimo, pero la mayoría de los sitios legítimos utilizan HTTPS porque es más seguro. Los sitios HTTP, incluso los legítimos, son vulnerables para los hackers.*
- *Si sospecha que un correo electrónico no es legítimo, seleccione un nombre o parte del texto del mensaje y llévelo a un motor de búsqueda para ver si existe algún ataque de phishing conocido que utiliza los mismos métodos.*
- *Pase el cursor del ratón por encima del enlace para ver si es legítimo.*

Llevando a cabo correctamente estas prácticas es un 99% seguro que no se tengan problemas de Phishing.

4.3 Aumentar la seguridad

Claramente todos estos tipos de ataques son generados comúnmente por errores a nivel usuario, navegación web sin control, descarga de archivos multimedia, descarga de programas piratas, etcétera. Todos estos problemas pueden ser controlados mediante políticas que se pueden generar ya sea en el dominio o en un Firewall, de igual forma el método más fuerte es capacitar a los usuarios para que tengamos una cultura informática dentro de la empresa y así los mismos usuarios puedan reconocer un comportamiento anormal dentro de sus equipos o reconocer un correo que contenga un virus y así poder informar al área de sistemas y puedan realizar los movimientos correspondientes.

4.3.1 Nivel Software

Para estar seguros a nivel software es recomendable tener en cuenta los siguientes puntos.

- Tener instalado software original con licenciamiento.
- Mantener un Antivirus con análisis o vigilancia en tiempo real.
- No instalar software de terceros.
- Capacitar al usuario final con conceptos técnicos.

4.3.2 Nivel Hardware

En el nivel hardware la seguridad para que un usuario no se lleve un dispositivo de almacenamiento o intente sacar información con algún dispositivo externo, se recomienda seguir los siguientes puntos.

- Bloquear los puertos USB de los equipos de cómputo.
- Tener un control del acceso al SITE.
- No permitir que el usuario realice modificaciones físicas a los equipos de cómputo.

Capítulo 5. Sistemas de respaldos

5.1 ¿Qué es un sistema de respaldos?

Es un sistema que consiste en el resguardo y encriptación de datos, que se encuentran almacenados en un equipo de cómputo.

5.2 ¿Para qué sirve un sistema de respaldos?

El sistema de respaldos funciona para las posibles catástrofes que un usuario puede tener en el mundo laboral, ya sea que un disco duro deje de funcionar, un virus infecto la información, secuestro de información, etcétera. Cuando estas catástrofes entran el sistema de respaldos facilitará la recuperación de los datos y así estar preparados para cualquier situación que se presente.

5.3 Mejores Sistemas de Respaldo

Los sistemas de Respaldo son limitados, ya que actualmente no se cuenta con gran diversidad de éste, por lo tanto, no existe una gran variedad y sus funciones son limitadas.

A continuación, se mencionará algunas opciones de sistemas de respaldo que se encuentran en la actualidad, en lo que personalmente cumplen con su función y siguen recibiendo actualizaciones para nuevas funciones.

5.3.1 EaseUs Todo

Es una solución de administración centralizada de copias de seguridad ayuda a desplegar tareas de copia de seguridad de uno o varios equipos desde una consola, ejecuta y supervisa copias de seguridad en todos los sistemas.

EaseUs es un software de paga el cual cobra por Equipo de Trabajo, Servidor y Servidor Avanzado, cuenta con una versión de prueba para que puedas explorar las diferentes funciones que aguarda este programa el cual tiene múltiples reseñas de diferentes editores y cuenta con más de 40 millones de usuarios.

Imagen 1. Logo EaseUS Recuperado de: https://es.easeus.com/ (fecha de recuperación: 11/03/2021)

5.3.2 Cobian Backup

Cobian Backup es un programa de respaldo de archivos que se puede utilizar para realizar respaldos automáticos de sus directorios y archivos. Cobian Backup se puede ejecutar como un servicio o como una aplicación normal. Puede hacer una copia de seguridad en otra ubicación en la misma computadora, a la red e incluso a un servidor FTP. El programa admite compresión y encriptación.

Cabe de destacar que Cobian, es un programa de código libre, el cual puede utilizarse incluso en un entorno comercial.

Lamentablemente CobianSoft se detuvo hasta su versión 11 ya que el código fuente fue vendido, pero no deja de ser una buena opción para iniciar un sistema de respaldos dentro de una empresa.

Imagen 2. Logo CobianSoft Recuperado de: https://www.cobiansoft.com/ (fecha de recuperación: 11/03/2021)

5.3.3 Areca Backup

Areca es una solución de respaldo de código abierto para Linux y Windows, el cual cuenta con formato de compresión, guardado de respaldo mediante FTP, Filtración de archivos, etcétera. Areca Básicamente, permite seleccionar un conjunto de archivos / directorios para hacer una copia de seguridad, elegir dónde y cómo (como una copia de archivo simple, como un archivo zip) se almacenará y configurará acciones posteriores a la copia de seguridad (como envío de informes de respaldo por correo electrónico o lanzamiento de scripts de Shell personalizados).

Imagen 3. Logo Areca Backup Recuperado de: http://www.areca-backup.org/ (fecha de recuperación: 11/03/2021)

5.3.4 Acronis

Acronis es un sistema de respaldos de paga el cual nos ofrece diversas opciones al contratar con ellos como almacenamiento en nube, infraestructura cibernética, o servicio de recuperación tras un desastre.

Pero el que nos interesa es Acronis BackUp, ya que es el sistema de respaldo que nos permite gestionar todos los equipos desde la consola del software, realizar planes inteligentes y direccionar el almacenamiento ya sea en la nube de Acronis, en un NAS o en ambos.

Acronis es una opción de paga, pero fiable ya que es uno del software líder de copia de seguridad respaldando información de clubes deportivos e integrando su software con grandes compañías como son Google, Microsoft, MariaDB, etcétera.

Imagen 4. Logo Acronis recuperado de: https://www.acronis.com/es-mx/ (fecha de recuperación: 11/03/2021)

5.3.5 ¿Cuál es la mejor opción?

Para elegir la mejor opción de sistemas de respaldos necesitamos comparar sus características.

	EaseUs Todo	Cobian Backup	Areca Backup	Acronis
Escalabilidad				x
Redundancia	x	x		x
Encriptación	x		x	x
Historial	x			x
Plan inteligente	x			x
Seguridad y fiabilidad.	x	x	x	x
Automatización	x			x
Interfaz intuitiva	x	x	x	x
Soporte Activo	x			x
Accesible	x	x	x	

Cuadro comparativo 1 sistemas de respaldo Fuente: Elaboración Propia.

Basado en este cuadro comparativo lo más lógico es basarse en el mejor software en este caso de los 4 mencionados sería Acronis o EaseUS Todo, pero en lo que realmente nos debemos de fijar es en la infraestructura que se tiene en la organización, ya que si no se tiene la infraestructura adecuada Acronis sería una implementación no útil y no se aprovecharía al 100%.

Hay puntos importantes que destacar al momento de elegir la mejor opción.

- Revisar bien la infraestructura con la que cuentas.
- Verificar cuanto ingreso dará la empresa para la implementación.
- Realizar un estudio de toda la cantidad de información que almacenaras

Capítulo 6. Acronis

Esta sección se centrará en Acronis ya que fue el sistema de respaldos que se utilizó en la empresa Excel Consultores, empresa dedicada al outsourcing.

6.1 ¿Qué es Acronis Management?

Como se mencionó en el capítulo Anterior Acronis es un sistema de respaldo Premium el cual tiene reconocimientos como el mejor software de Japón o premio ITReview grid, todo esto por su gran sistema de respaldos.

Algunas de sus Características más destacadas son las siguientes:

- Protección proactiva contra Ransomware.
- Instant Restore.
- Protección completa.
- 0% de falsos positivos.
- Arquitectura de cloud híbrido.

6.2 ¿Por qué se eligió Acronis?

Acronis puede tener la imagen del mejor software de sistemas de respaldo, no se seleccionó simplemente por eso, se eligió Acronis por la gran cantidad de información que se tiene en la organización que se elabora, es decir más de 10 TB de información y más de 200 Equipos de Cómputo, por lo cual Acronis cumple y soporta la gran cantidad de Equipos de Cómputo y Servidores que se necesitan respaldar.

6.3 Experiencia personal al trabajar con Acronis Management

La experiencia al trabajar con Acronis es satisfactoria, ya que el sistema es muy intuitivo, pero al mismo tiempo es muy avanzado, ya que, desde la consola, se puede planificar y monitorear el proceso de los respaldos, de igual forma permite modificar cuanto recurso va a utilizar el programa para realizar el respaldo, se puede configurar el destino del respaldo, etcétera. La empresa de Acronis mantiene con actualizaciones activas y sigue teniendo un perfecto soporte técnico, a pesar de que se han encontrado errores dentro del sistema, Acronis han podido otorgar soluciones y continuamente sacan diferentes modalidades de respaldos.

Los puntos malos de Acronis son que, si la organización u empresa no tiene la infraestructura correcta para soportar el sistema de Acronis, será difícil poderlo trabajar al 100% y existirán retrasos con los equipos de cómputo, en este ámbito Acronis si es muy estricto, de modo que los ingenieros que dan soporte hablan totalmente en idioma inglés.

Se puede decir que Acronis es la mejor opción de sistemas de respaldo, siempre y cuando se tenga la infraestructura para soportar dicho sistema y que el ingeniero que administre el sistema de respaldos tenga un gran conocimiento del sistema ya que, es fácil de usar, pero tiene opciones muy avanzadas que pueden ayudar que el sistema sea autónomo.

Caso Práctico. Implementación del correcto control de respaldos con Acronis Management para usuarios finales

Instalación de la consola de Acronis Managment

Antes de iniciar con la instalación de Acronis se debe de tener en cuenta los requisitos mínimos que se necesitan en el servidor principal los cuales, según Acronis Managment son los siguientes:

- 4 CPU lógicas
- 4 GB de RAM
- Interfaz de red de 1 GbE con una dirección IP estática. También puede usar la misma interfaz de red para el tráfico interno y externo (pero se recomienda que configure una red segura más tarde).

¿Dónde descargarlo?

El instalador del software se otorga mediante la página de Acronis en el instante de adquirir el producto, también se puede obtener mediante el proveedor en el cual se adquirió el servicio.

Instalación de la Consola de Acronis

Para realizar esta instalación es necesario tener levantado un servidor con el sistema operativo Windows Server ya que este ejercicio se llevará a cabo mediante ese ambiente.

Una vez descargado el cliente en el servidor es importante aceptar los términos y condiciones de la licencia como lo muestra la siguiente imagen (Imagen 5, Contrato de licencia).

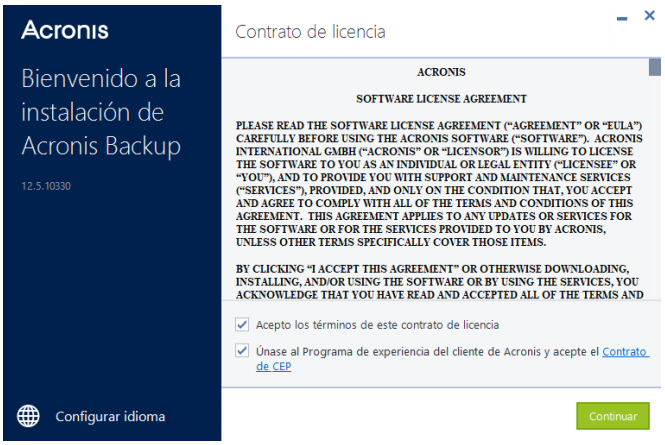

Imagen 5. Contrato de licencia. Recuperado de: Software Acronis, 20/05/2022.

Después de aceptar los términos de condiciones mostrara la siguiente ventana (Imagen 6. Instalación Acronis)

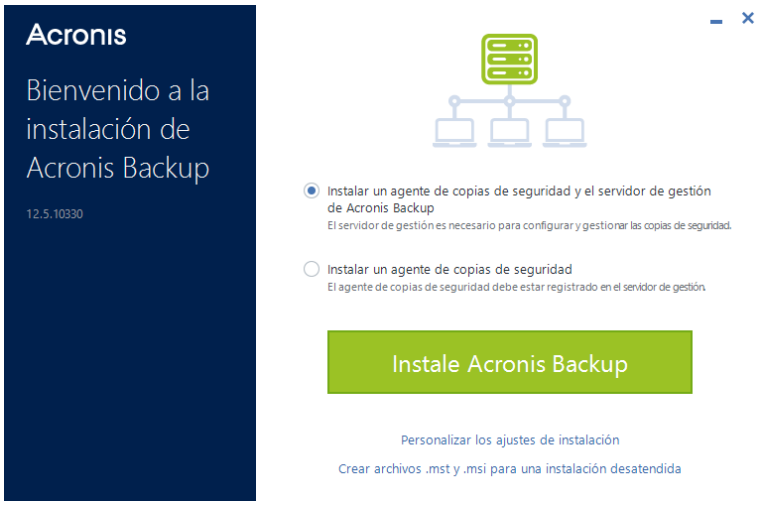

Imagen 6. instalación Acronis. Recuperado de: Software Acronis, 20/05/2022.

Esta ventana muestra desde el ejecutable las opciones de instalación, como se puede ver en la primera opción se tiene el proceso para instalar el gestor de servidor de Acronis Backup, el cual es el que requiere antes de instalar un agente de copias de seguridad.

Se selecciona la opción de Personalizar los Ajustes de instalación, ya que es necesario crear una cuenta en específico para el administrador de Acronis, para eso se entra a los ajustes de instalación (Imagen 7. Ajustes de instalación.)

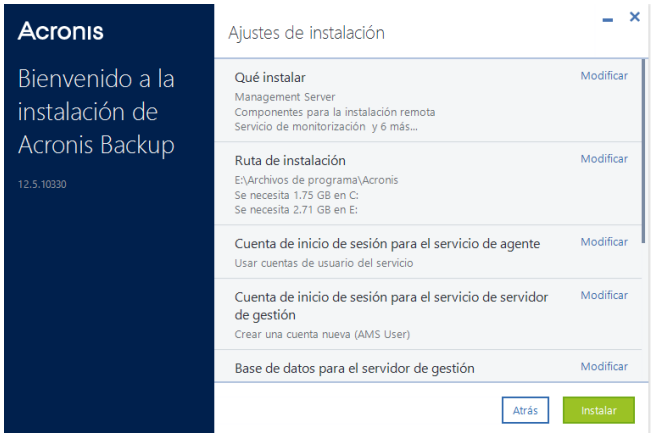

Imagen 7. Ajustes de instalación. Recuperado de: Software Acronis, 20/05/2022.

Desde la opción seleccionada, se puede establecer parámetros antes de realizar la instalación de la consola de Acronis los cuales son los siguientes:

- Que instalar
- Donde se va a instalar
- Cuenta de administrador
- Bases de datos para el servidor de gestión
- Puertos HTTP
- Puertos TCP
- Puesto o dirección IP del servidor
- Servidor Proxy HTTP

Primero se da clic en la cuenta de inicio de sesión para el servidor de agente y mostrará lo siguiente (Imagen 8 Cuenta de inicio de sesión).

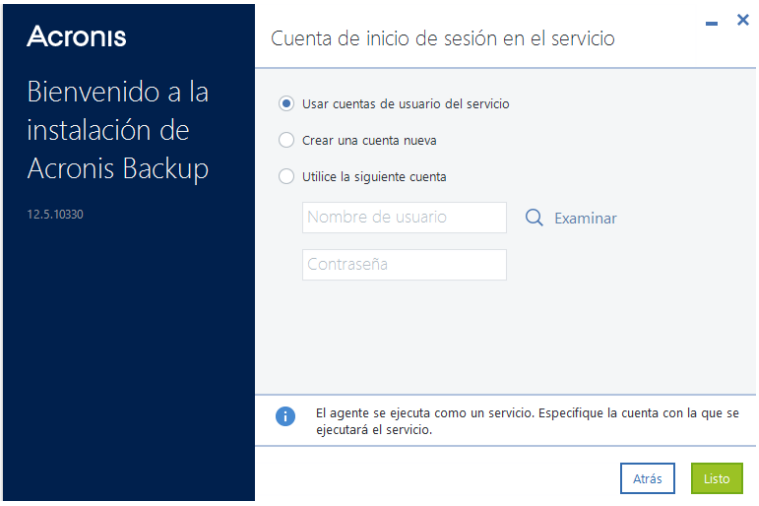

Imagen 8. Cuenta Inicio de sesión. Recuperado de: Software Acronis, 20/05/2022.

Se tienen 3 opciones para seleccionar que es lo que vamos a hacer para iniciar sesión en la consola de Acronis, solamente se tomarán dos en cuenta, la opción de crear una cuenta nueva y Utilice la siguiente cuenta.

Se utilizarán las siguientes cuentas ya que la primera opción toma la cuenta del equipo en el que está instalando el servicio de Acronis, en este caso es el servidor y no es recomendable tener las mismas credenciales de acceso en más de un sistema por seguridad de la información.

En este caso se selecciona “Utilice la siguiente cuenta y se le da clic al botón de examinar y aparecerá la siguiente ventana (Imagen 9 Alta de cuenta).

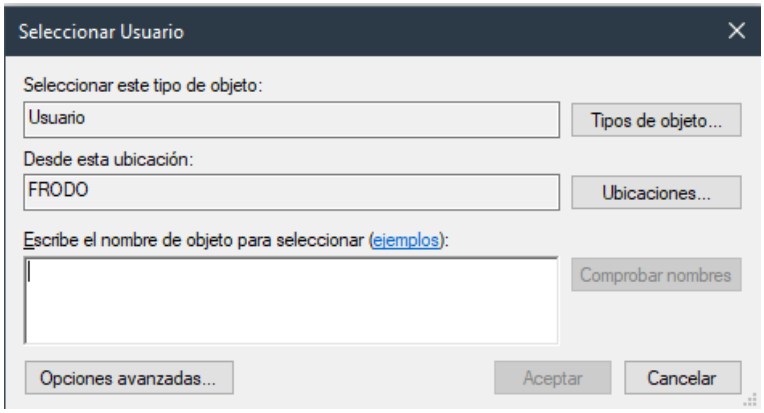

Imagen 9. Alta cuenta. Recuperado de: Software Acronis, 20/05/2022.

Esta ventana es la que se utilizará para buscar un usuario dentro de un dominio en el Active directory, por lo tanto, tiene las mismas funciones. Se introduce el usuario que se desea que tenga el acceso a la consola y dar clic en comprobar nombres, una vez comprobado el nombre se acepta y automáticamente el instalador muestra el Dominio y el usuario (Imagen10. Asignación cuenta de inicio de sesión).

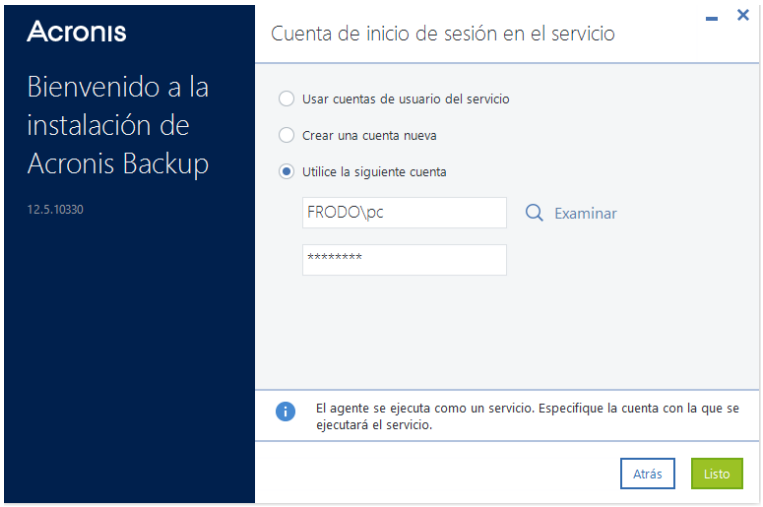

Imagen 10. asignación cuenta de inicio de sesión. Recuperado de: Software Acronis, 20/05/2022.

Ahora se configurará la dirección IP de la consola de Acronis, se desplaza con la barra de navegación los ajustes de instalación y seleccionar el nombre o la dirección IP del servidor de gestión.

Una vez dentro de la modificación de esta área mostrará la siguiente pantalla (Imagen 11. Asignación de dirección IP).

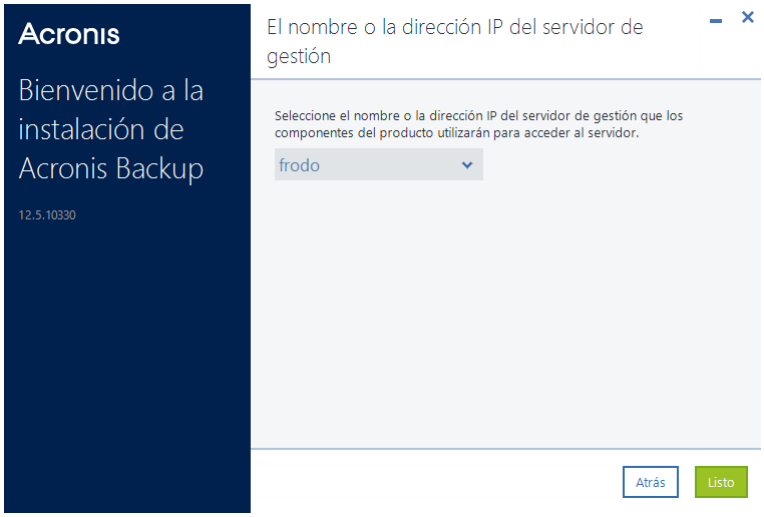

Imagen 11. asignación de dirección IP. Recuperado de: Software Acronis, 20/05/2022.

Se da clic la barra desplazadora que nos muestra el instalador y seleccionar la dirección IP del servidor en el que se está instalando.

Una vez terminado la instalación del Panel de control del sistema de Acronis Managment mostrará la dirección de la consola web en la cual se puede configurar todos los servicios que ofrece el sistema de respaldo.

Una vez finalizado la configuración de la instalación de la consola de Acronis, aparecerá la siguiente pantalla donde el cliente de instalación informará que ésta es correcta (Imagen 12. Instalación Correcta).

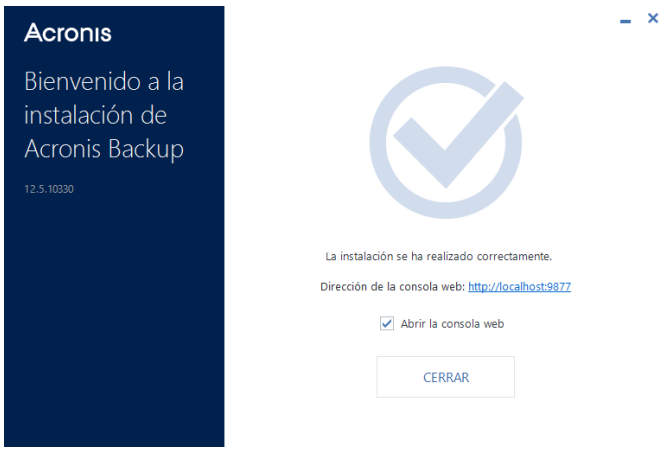

Imagen 12. Instalación Correcta. Recuperado de: Software Acronis, 20/05/2022.

Como usuario local podemos ingresar desde la dirección que muestra al finalizar la instalación, pero si se desea ingresar desde otro equipo del mismo dominio hay que recordar que la dirección de nuestro servidor IP y el puerto de enlace que nos otorga por default que es el 9877.

Entonces el enlace para el ingreso afuera del servidor seria la Dirección IP del servido más el puerto de entrada (192.168.1.1:9877)

Una vez introducido esta dirección IP abrirá la interfaz web de la consola de Acronis y mostrará un login (Imagen 13. Login Consola Acronis).

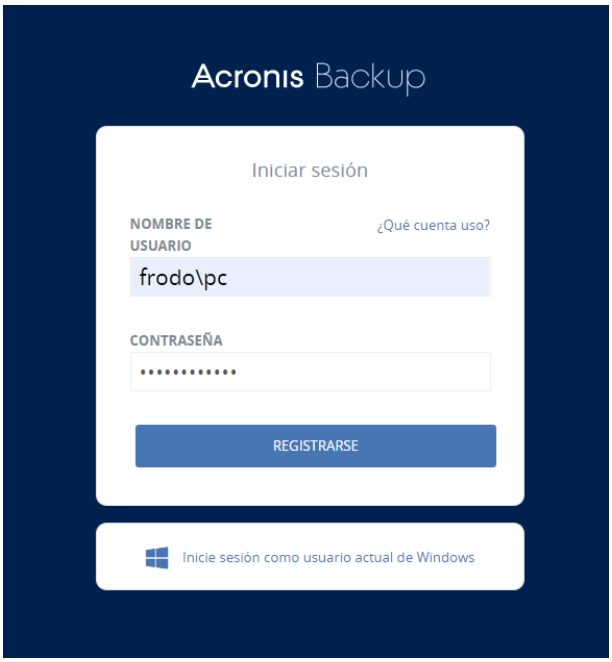

Imagen 13. Login Consola Acronis. Recuperado de: Software Acronis, 20/05/2022.

Se inicia sesión y ya se visualizará la consola corriendo correctamente (Imagen 14. Interfaz Acronis).

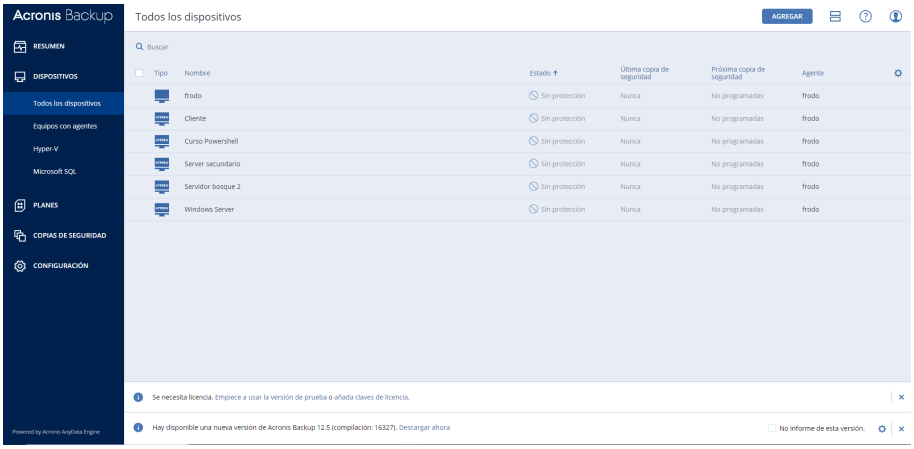

Imagen 14. Interfaz Acronis. Recuperado de: Software Acronis, 20/05/2022.

En este método se instala de forma correcta la consola de Acronis Managment.

Creación de unidad la Consola de Acronis e instalando clientes de Acronis

Después de la instalación de la consola de Acronis, se empezará con la configuración de ésta, con el objetivo del momento al unir un equipo a la consola ya tenga el conocimiento el cliente de Acronis y así saber que procesos realizar.

Crear una Unidad

Las unidades de Acronis son los repositorios donde se crear un grupo de equipo en el cual se establece como, cuando y donde se realizará el plan de respaldo del equipo de cómputo, por lo tanto, es importante de crear para el correcto control de respaldos.

Una vez dentro de la consola en la opción de Configuración en el cual permite realizar muchas acciones, una de ellas es administrar las unidades que tenemos dentro de la consola y a los administradores que se agreguen como se muestra en la siguiente imagen (Imagen 15. Opción Administradores.)

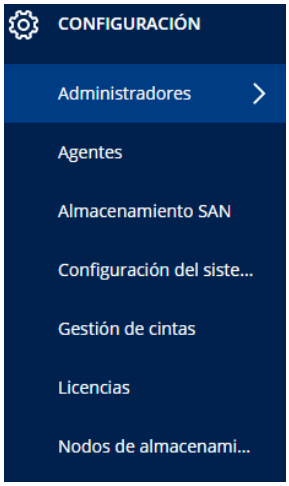

Imagen 15. Opción Administradores. Recuperado de: Software Acronis, 20/05/2022.

Dentro de la opción Administradores se visualiza la siguiente pantalla (Imagen 16. Unidad).

Imagen 16. Unidad. Recuperado de: Software Acronis, 20/05/2022.

Dentro de la pantalla mencionada se da clic en Crear Unidad y al momento de crear la unidad mostrará la opción para renombrar la unidad (Imagen 17. Crear Unidad).

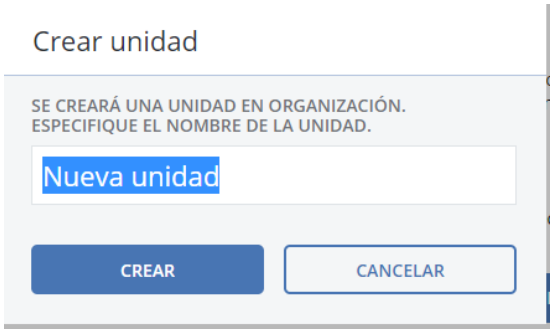

Imagen 17. Crear Unidad. Recuperado de: Software Acronis, 20/05/2022.

Una vez creada la Unidad mostrara la unidad creada y los administradores que componen a la unidad, por el momento la unidad creada se encuentra vacía ya que no contiene ningún equipo asignado como lo muestra la siguiente imagen (Imagen 18. Organizaciones).

Imagen 18. Organizaciones. Recuperado de: Software Acronis, 20/05/2022.

Instalación de Clientes

Una vez creado la unidad en la consola de Acronis, es necesario instalar los clientes antes de crear el plan de respaldos.

Quizás se puede preguntar ¿a qué se refiere con clientes? En este punto, los clientes en el sistema de Acronis son todos los Equipos de cómputo que se respaldaran. A continuación, ejecutamos el exe que Acronis otorga para la instalación de clientes, normalmente es el mismo ejecutable con el que instalamos la consola de Acronis.

Una vez ubicados el equipo o los equipos que se realizará el respaldo de información se ejecuta el programa de Acronis, aceptando los términos y

condiciones del software. Una vez terminado, mostrará la siguiente imagen (Imagen 19. Instalación del Cliente).

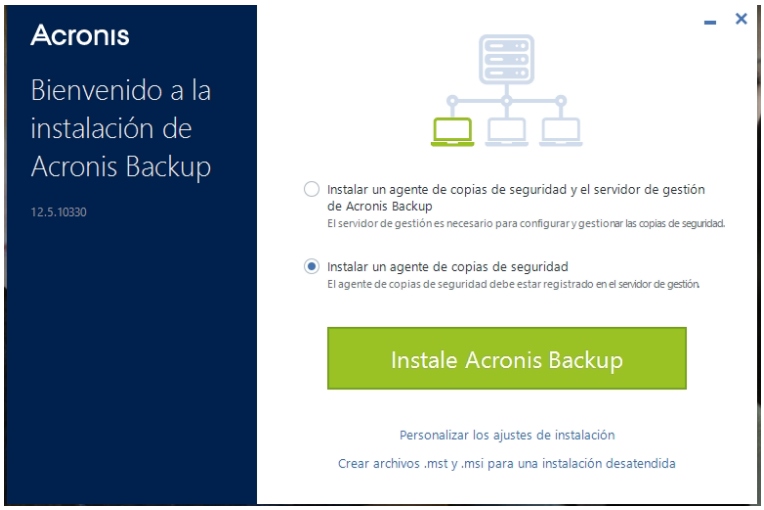

Imagen 19. Instalación de Cliente. Recuperado de: Software Acronis, 20/05/2022.

En esta sección, se selecciona la opción “Instalar un agente de copias de seguridad” y se da clic en el botón verde para empezar con la instalación de del Cliente.

A continuación, mostrará la siguiente imagen (Imagen 20. Direccionar el servidor de respaldo) en la cual solicita la dirección IP del servidor en la cual se encuentra instalado la consola de Acronis.

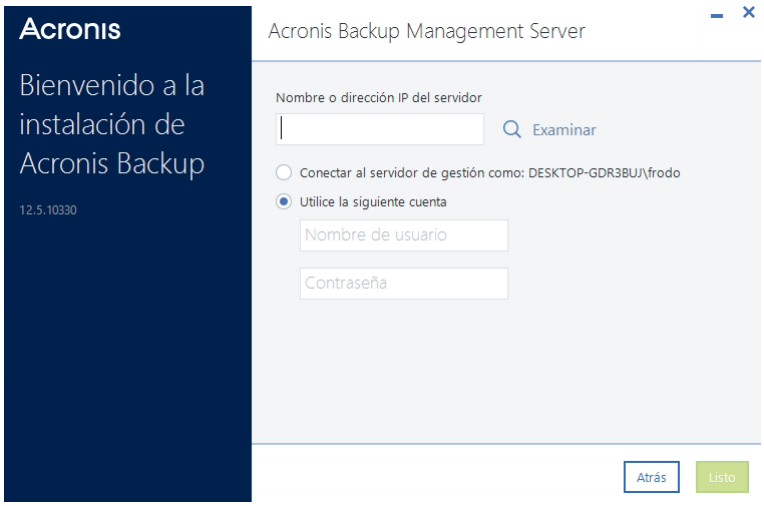

Imagen 20. Direccionar al Servidor de respaldo. Recuperado de: Software Acronis, 20/05/2022.

En la sección actual se debe de introducir la dirección IP en la que se encuentra ubicado la consola de Acronis, en este caso la dirección que se asignó fue 192.168.100.10:9877, una vez declarando el Nombre o dirección IP del servidor, se selecciona la opción llamada “Utilice la siguiente cuenta” ya que como el equipo en el que se encuentra no tiene permisos sobre el servidor de Respaldos es imposible conectarse al servidor de gestión con las credenciales del cliente, por lo tanto al seleccionar la opción mencionada, se ingresa manualmente el usuario y contraseña del servidor de respaldos y así el cliente puede autentificarse y establecer una conexión. Una vez introducido los valores requerido damos clic en “Listo” y mostrará la siguiente imagen (Imagen 21. Selección de Organización).

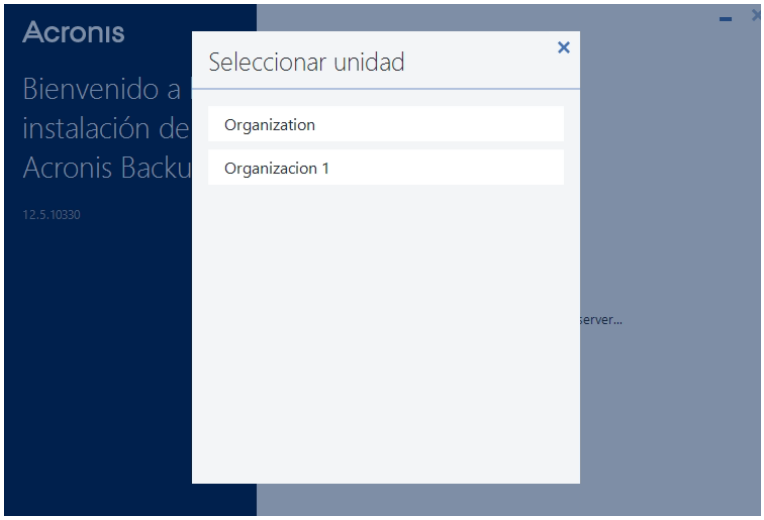

Imagen 21. Selección de Organización. Recuperado de: Software Acronis, 20/05/2022.

Esta sección es importante, ya que retomando los pasos anteriores creamos las Organizaciones, en este punto se decide donde el cliente va a estar ubicado dentro de la consola de Acronis, se puede seleccionar desde la organización raíz que es donde se podrá asignar el equipo a cualquier organización en un futuro o seleccionar una organización en específico que se requiera.

Una vez seleccionando la Organización, el cliente empezará con la instalación como se muestra la siguiente imagen (Imagen 22. Instalación de Cliente).

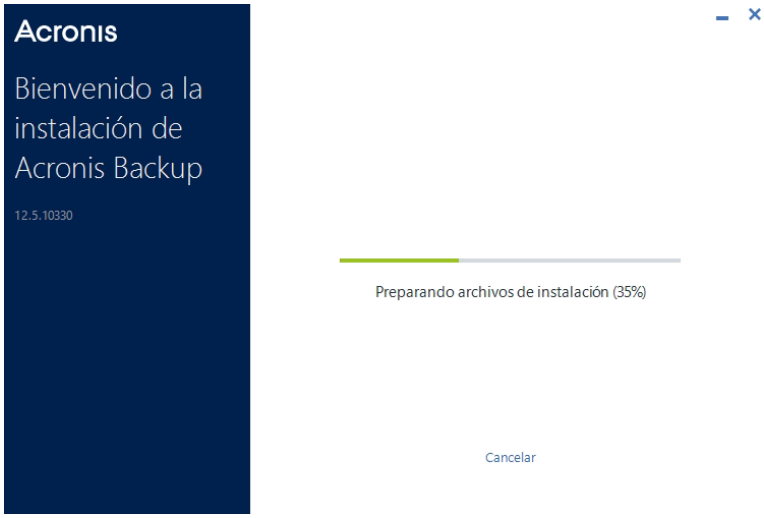

Imagen 22. Instalación de Cliente. Recuperado de: Software Acronis, 20/05/2022.

Al momento de que finalice mostrará la siguiente imagen (Imagen 23. Instalación del Cliente)

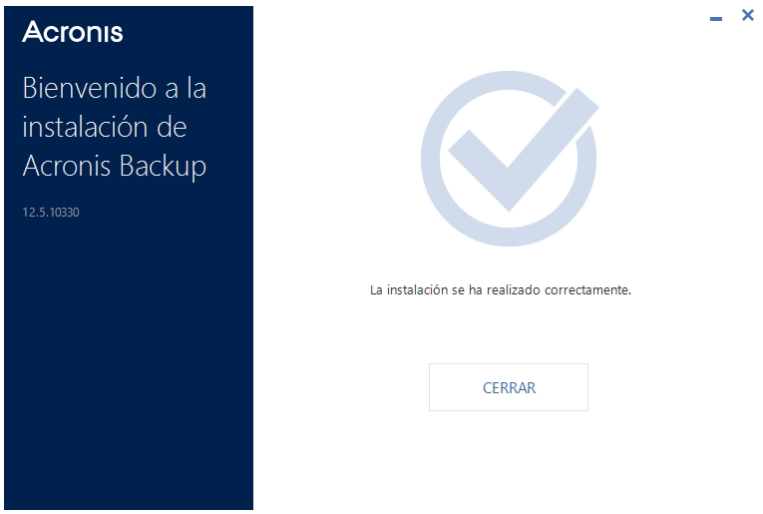

Imagen 23. Instalación del Cliente Completa. Recuperado de: Software Acronis, 20/05/2022.

De igual forma en la sección de íconos ocultos se encuentra el icono de Acronis en el cual muestra como está activo y en proceso.

Creación de un correcto plan de respaldo.

En este punto se regresa a la consola de Acronis ya que instalado el cliente y creando la unidad de respaldos en la consola de Acronis es posible seleccionar una unidad en especifica o de lo contrario la organización completa, en la parte superior izquierda de la consola permite realizar dicha acción (Imagen 24. Creación de un plan de respaldo).

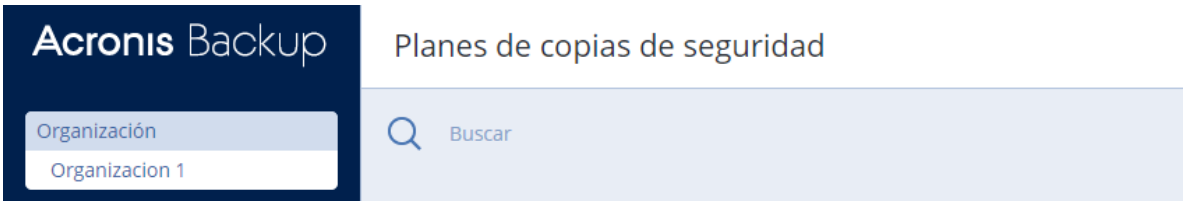

Imagen 24. Creación de un plan de respaldo. Recuperado de: Software Acronis, 20/05/2022.

Se selecciona la unidad creada y en el menú desplegable seleccionamos la opción “Planes”.

Una vez seleccionada la opción de Planes despliega una lista de proceso que se pueden realizar (Imagen 25. Crear copia de seguridad), el proceso que se utilizara para realizar respaldos autónomos es la primera opción llamada “Crear Copia de Seguridad”. Esta opción permite realizar la creación de planes autónomos en el cual conforme diga el plan el respaldo autónomo se realizará para los equipos asignados.

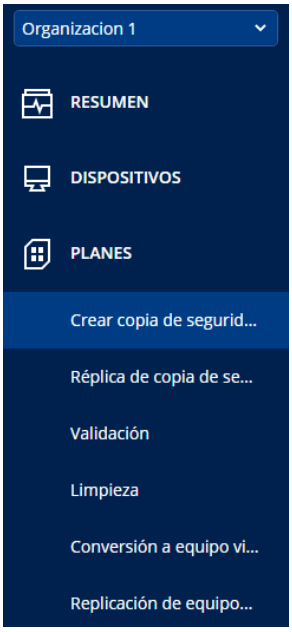

Imagen 25. Crear copia de seguridad. Recuperado de: Software Acronis, 20/05/2022.

Una vez seleccionada la opción “Crear Copia de Seguridad” mostrará una nueva pantalla en la cual mostrara todos los planes que se han creado en la Organización 1, pero como aún no se crea ningún plan se muestra vacía la sección y solamente se aprecia el botón de crear plan en la parte superior derecha de la consola (Imagen 26. Botón Crear Plan).

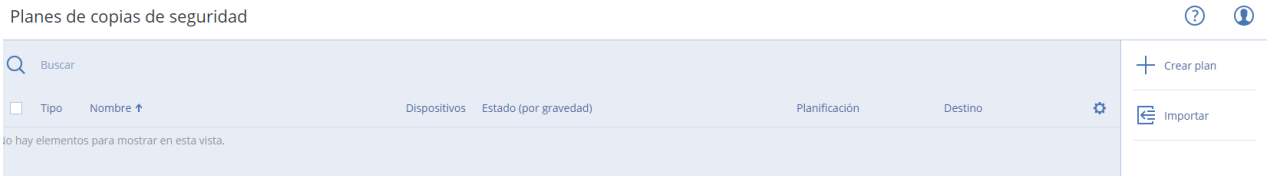

Imagen 26. Botón Crear Plan. Recuperado de: Software Acronis, 20/05/2022.

Se selecciona el botón de crear plan, el cual muestra todas las configuraciones que se pueden realizar un plan de respaldo (Imagen 27. Opciones de Plan de seguridad).

Imagen 27. Opciones de Plan de seguridad. Recuperado de: Software Acronis, 20/05/2022.

En cualquier plan de respaldo que se cree, se debe de identificar con una nomenclatura que se maneje en la organización donde se elabore. El primer paso para crear un correcto plan de respaldo es identificar y personalizar el plan de respaldo, así que al dar clic en el lápiz ubicado en la parte superior se mostrará la opción para cambiar el nombre del Plan de respaldo (Imagen 28. Nombre del plan.)

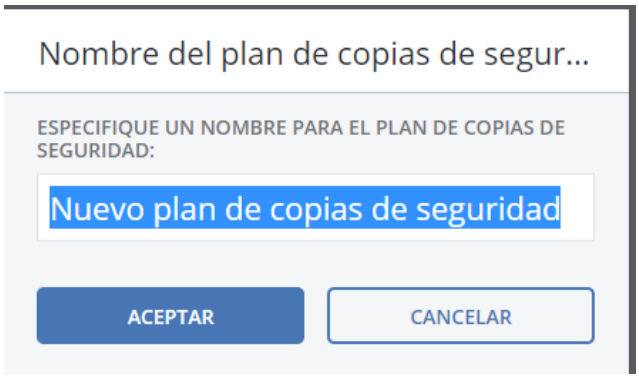

Imagen 28. Nombre del plan. Recuperado de: Software Acronis, 20/05/2022.

Opciones de copia de seguridad

Las opciones de seguridad son importantes en el plan de respaldo, ya que desde a estas opciones se puede manejar el nivel de comprensión del respaldo que se realizara, script para el funcionamiento de Acronis o el nivel de recursos que se le da a la operación. Para este caso se tomarán solamente dos opciones de las diversas que tiene el programa ya que solamente son necesarias para lograr lo planteado en la Hipótesis.

Nivel de Comprensión

La opción de Nivel de Comprensión permite reducir el tamaño de almacenamiento del respaldo de un equipo de cómputo, si un respaldo pesa 50 GB y el nivel de comprensión esta al máximo el tamaño total del respaldo realizado es de 25 GB.

Por lo tanto, la opción de nivel de comprensión contiene 4 niveles.

- Ninguno
- Normal
- Alto
- Máximo

La diferencia de estos 4 niveles es la siguiente, entre más alto sea la comprensión del respaldo el tiempo de proceso es más largo, por lo tanto al realizar un respaldo de información con un nivel de comprensión al máximo es demasiado tardado pero el más correcto ya que al llevar el correcto control de respaldos de la información también se debe de llevar un correcto control de almacenamiento y si Acronis permite minimizar el almacenamiento de un equipo que contiene mucha información mejor para nuestro servidor de respaldos, se selecciona el nivel de comprensión más alto con el fin de que no se ocupe mucho espacio en el NAS (Imagen 29. Nivel de comprensión.).

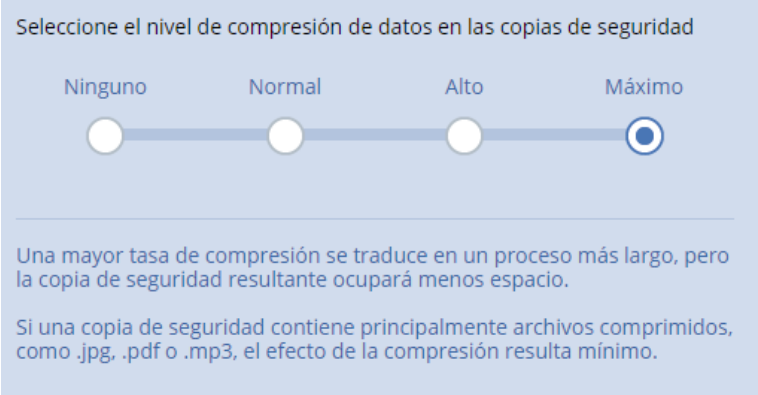

Imagen 29. Nivel de compresión. Recuperado de: Software Acronis, 20/05/2022.

Rendimiento

La opción de rendimiento permite dar prioridad al proceso que se ejecuta al realizar el respaldo de información, esto afectara a los recursos del equipo que se está respaldando en otras palabras entre más Alta sea la prioridad del proceso más recursos del equipo de cómputo utiliza. La opción mencionada otorga 3 niveles de rendimiento.

- Bajo
- Normal
- Alto

De igual forma da una opción de porcentaje de salida de datos mediante el cliente de Acronis esta opción es utilizada cuando se requiere realizar un respaldo mientras el usuario utiliza el equipo de cómputo, con el fin de que al momento que se ejecute el proceso de respaldo no se vea afectada la experiencia del usuario mientras esta activo en el equipo.

La opción correcta de esta sección depende ya del criterio del ingeniero a cargo, ya que cada equipo de cómputo es diferente tanto se pueden tener gamas altas o gamas medias de equipos, lo recomendable es tenerlo en un rendimiento normal siempre y cuando las especificaciones del equipo de cómputo a respaldar sean en

gama media, o al contrario, si las especificaciones del equipo de cómputo son altas aumentar el rendimiento a nivel alto, en la práctica actual se selecciona la opción normal (Imagen 30. Prioridad del Proceso.).

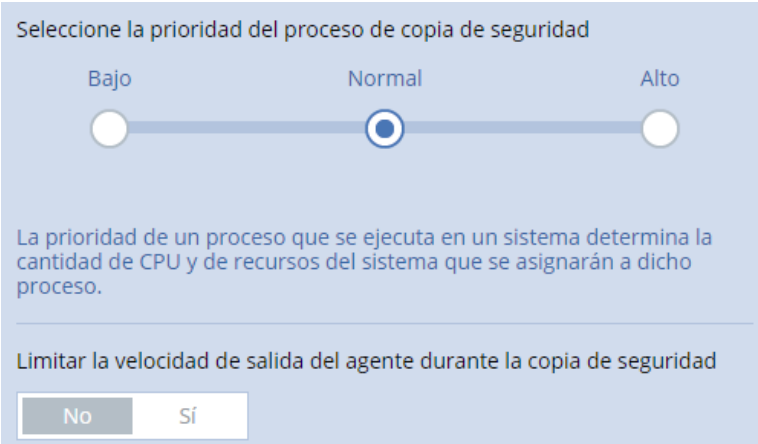

Imagen 30. Prioridad del Proceso. Recuperado de: Software Acronis, 20/05/2022.

Que incorpora la copia de seguridad

En la siguiente sección se seleccionará el tipo de respaldo de información se incorporará o se asignará a los clientes.

La única diferencia de todas las opciones que tenemos en Acronis es el tipo de información que se respaldará o realizar el respaldo de Discos/Volúmenes o Archivos/Carpetas específicos, al momento de seleccionar estas opciones nos permitirá seleccionar específicamente que es lo que queremos respaldar, en este caso seleccionaremos todo el equipo (Imagen 31. Tipo de respaldo), porque lo que se busca es respaldar todo el equipo de cómputo o crear una imagen idéntica del cliente.

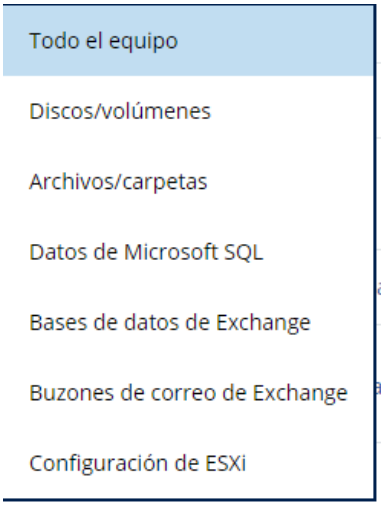

Imagen 31. Tipo de Respaldo. Recuperado de: Software Acronis, 20/05/2022.

Dispositivos

En la sección de dispositivos es donde mostrara todos los equipos que ya se instaló y configuró el cliente de Acronis Management.

Al dar clic en la opción mencionada, mostrara la siguiente pantalla, en la pantalla actual muestra si ya hay dispositivos agregados o de lo contrario tiene la opción de agregar, se da clic en el botón de agregar (Imagen 32. Dispositivo).

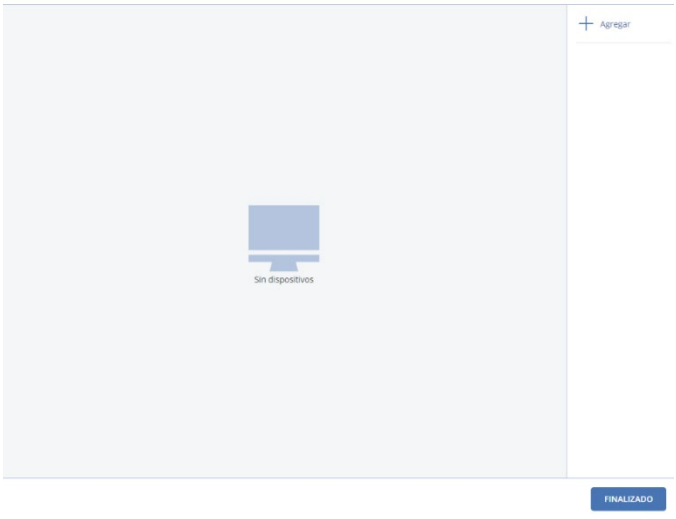

Imagen 32. Dispositivos. Recuperado de: Software Acronis, 20/05/2022.

Una vez accionado el botón se visualiza los clientes que están en la misma red, pero no tienen un plan asignado (Imagen 33. Agregar Dispositivo).

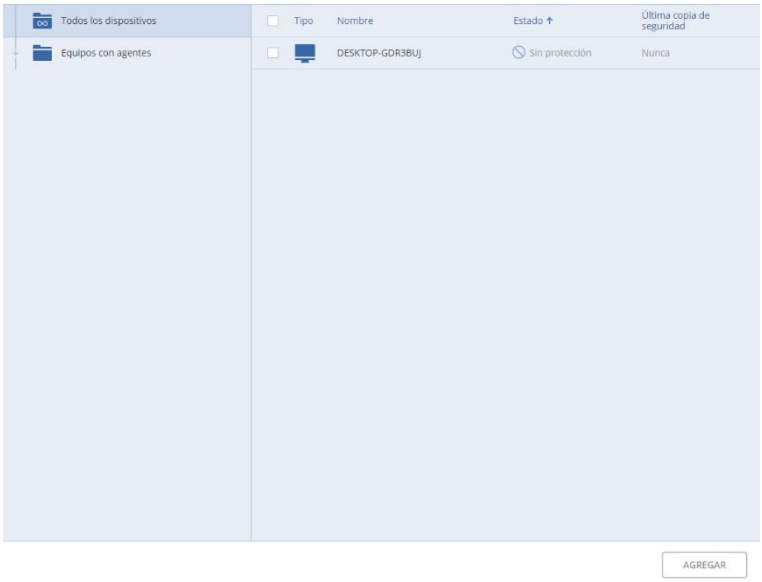

Imagen 33. Agregar Dispositivo. Recuperado de: Software Acronis, 20/05/2022.

En esta sección muestra los clientes o agentes que tenemos instalados en los equipos a respaldar, mostrando información básica, como: Tipo, Nombre, Estado, Ultima copia de seguridad.

Esta información es importante porque el tipo de equipo, ya que recordando no solamente se respondan equipos de cómputo también servidores o NAS, en nombre es recomendable llevar las buenas prácticas y tener una nomenclatura con los equipos de cómputo para ser capaces de identificarlos, en la sección de estado muestra si ya cuenta con un plan de respaldo y ultima copia de seguridad muestra la fecha de la última copia de seguridad que se realizó al equipo de cómputo. Se selecciona el equipo de cómputo y se acciona el botón de Agregar.

Una vez agregado el equipo de cómputo, mostrará que el equipo ya está asignado en el plan que se está creando.

Donde se guardarán las copias de seguridad

En esta sección se especifica en donde se guardará los respaldos, por falta de infraestructura en el laboratorio donde se está realizando estos ejemplos no contamos con un NAS activo, por lo tanto, se utilizará el almacenamiento local del equipo.

Se selecciona la opción y muestra las diferentes opciones para que se le indique al plan de respaldos donde almacenara los archivos (Imagen 34. Opción Copias de Seguridad).

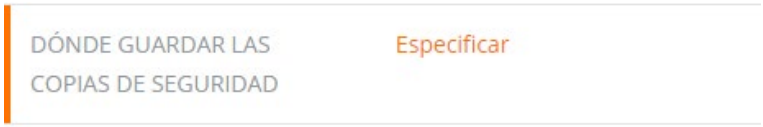

Imagen 34. Opción Copias de Seguridad. Recuperado de: Software Acronis, 20/05/2022.

Por lo mencionado anteriormente, se utiliza la carpeta local (Imagen 35. Selección de ubicación de respaldo) el cual muestra los volúmenes que tiene el equipo de cómputo, para almacenar el respaldo en un NAS se encuentra la opción de Carpetas de Red la cual se indica a la opción la dirección IP del NAS y la carpeta de red que se crea dentro del mismo y así almacenar todo mediante red.

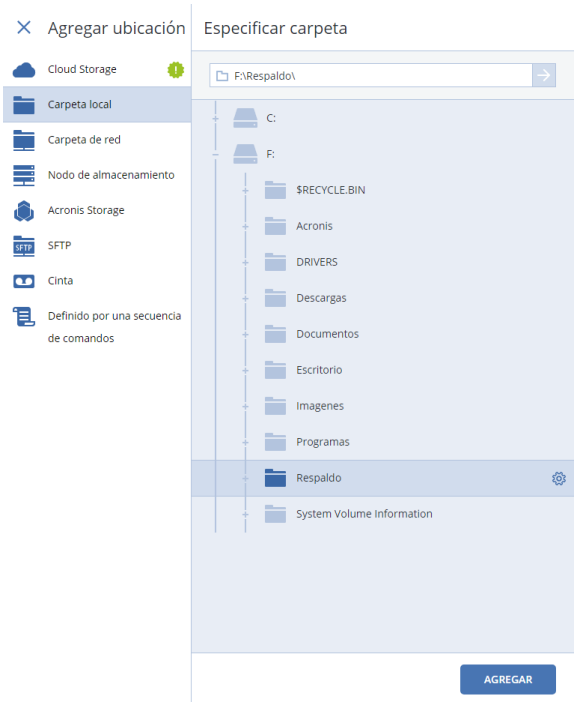

Imagen 35. Selección de ubicación de respaldo. Recuperado de: Software Acronis, 20/05/2022.

Planeación

La siguiente sección es planificación

Planificación es la opción donde se programará que días se realizará el respaldo del cliente (Imagen 36. Planificación.).

Imagen 36. Planificación. Recuperado de: Software Acronis, 20/05/2022.

El esquema de respaldos que se utilizará es incremental (Imagen 37 Esquema de copia de seguridad.), ya que el respaldo incremental solamente copia

los datos que han variado desde la última vez respaldado, por lo cual con este esquema se administrará de forma correcta el almacenamiento del servidor de respaldos.

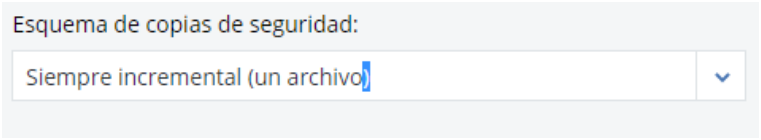

Imagen 37. Esquema de copia de seguridad. Recuperado de: Software Acronis, 20/05/2022.

Después sigue la planeación de cuándo y a qué hora se realizará el respaldo (Imagen 38 Planificación del respaldo), se utilizará el respaldo semanal y se realizará sábados y domingos en donde la operación es mínima o nula en los clientes, el respaldo empezará a medianoche, recordando que es incremental el esquema hay que tener en cuenta que el primer respaldo siempre será completo, los demás respaldos solamente guardarán los nuevos archivos que detecte el cliente de Acronis.

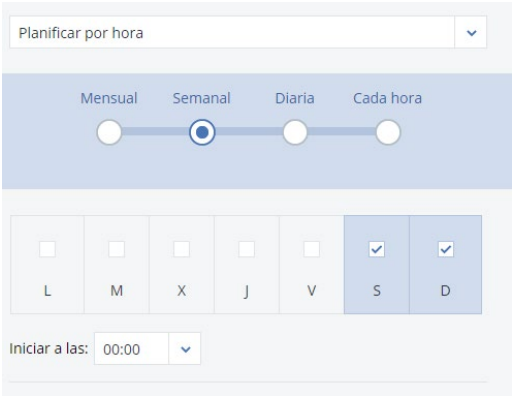

Imagen 38. Planificación del respaldo. Recuperado de: Software Acronis, 20/05/2022.

A continuación, se declaran las condiciones antes de que se realice el respaldo de información (Imagen 39. Condiciones de respaldo.). Normalmente los usuarios están acostumbrados a apagar el equipo de cómputo los fines de semana, por lo tanto, los equipos que se encuentran apagados no se respaldan para evitar

los incidentes causados a dicha acción, se selecciona la primera opción ya que al momento de encender el equipo permite realizar las tareas perdidas de Acronis.

La segunda opción nos permite evitar cualquier hibernación o suspensión del cliente, ya que, si los clientes entran en este estado, pueden dejar de enviar energía en periféricos importantes, uno de ellos el Disco Duro.

La tercera opción se selecciona ya que puede existir usuarios que suspendan el equipo de cómputo manualmente, para esto la tercera opción apoya en el que momento de que sea media noche y encuentra un equipo de cómputo en suspensión el proceso de respaldo reactive todo el cliente para que pueda realizar el proceso.

La condición de inicio que se marcara será que el usuario este inactivo, a partir de los 5 minutos de inactividad el plan entrara en acción.

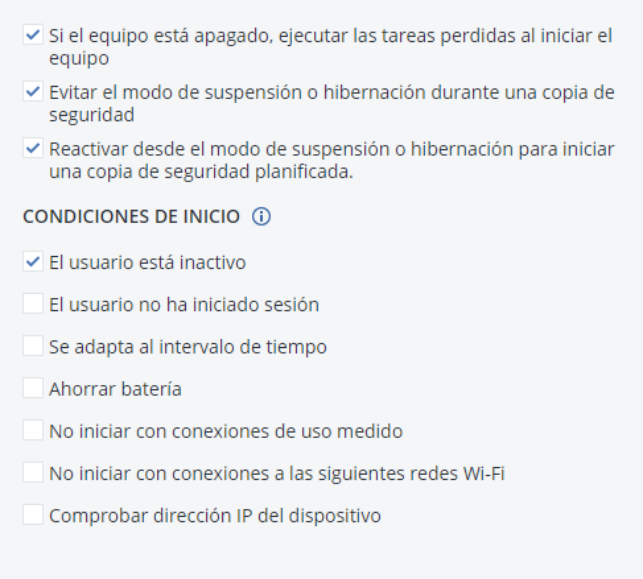

Imagen 39. Condiciones del respaldo. Recuperado de: Software Acronis, 20/05/2022.

Limpieza

En la opción de limpieza se programa automáticamente la limpieza del NAS o servidor de respaldos, dependiendo de la situación y de la capacidad del NAS activo es como se puede planificar la limpieza de este, la consola de Acronis muestra tres opciones (Imagen 40 Planificación de la limpieza.).

Por antigüedad. En esta sección se programa cuanto tiempo se desea que se almacene los archivos de respaldos

Número de Copias de Seguridad. Número de copias de seguridad permite establecer un límite de archivos de respaldos dentro del servidor.

Indefinido. No realiza ninguna acción de limpieza.

En este caso se selecciona por antigüedad ya que el almacenamiento del NAS es limitado y es necesario la administración de almacenamiento dentro del NAS.

Imagen 40. Planificación de la limpieza. Recuperado de: Software Acronis, 20/05/2022.

Cifrado

El cifrado en nuestros archivos de respaldo es importante y más si se desea que la empresa este trabajando sobre una normativa y por cuestiones de seguridad (Imagen 41. Opción de Cifrado.)

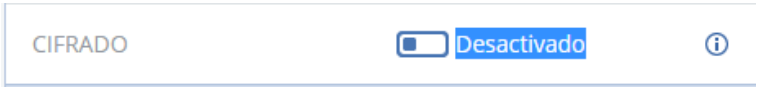

Imagen 41. Opción de Cifrado. Recuperado de: Software Acronis, 20/05/2022.

Al activarlo Acronis solicita una contraseña para los cifrados de los respaldos que se realizan y también podemos elegir el algoritmo que se aplica dentro del cifrado, en este caso se elegirá el algoritmo de cifrado 256 ya que el algoritmo 256 es un estándar de cifrado del gobierno de estados unidos y este aplica a documentos que pueden ser clasificados top secret (Imagen 42. Contraseña de Cifrado.)

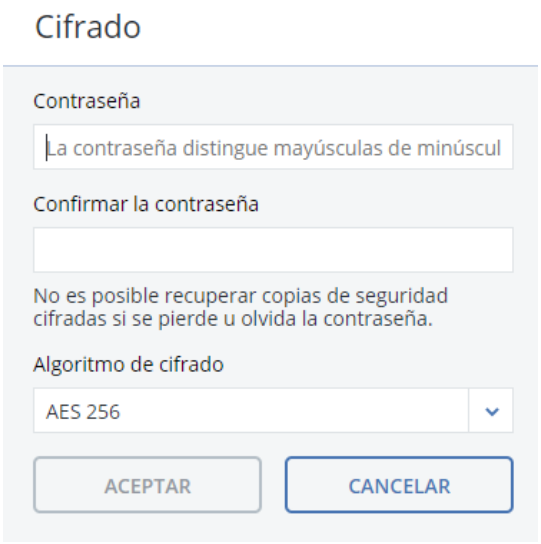

Imagen 42. Contraseña de Cifrado. Recuperado de: Software Acronis, 20/05/2022.

Segunda Ubicación

Antes de finalizar y crear el plan de respaldo, Acronis da la opción de agregar una segunda ubicación con el fin de tener un segundo respaldo, también la segunda ubicación permite realizar el tiempo de conservación de los archivos de respaldo.

Una vez finalizado todos los pasos anteriores, se da clic al botón de Crear (Imagen 43 y finalmente tenemos un plan inteligente y autónomo de respaldos, el cual respaldará la información de los clientes incrementalmente con condiciones de inicio siempre y cuando el equipo este inactivo y no entre en suspensión, en caso de que se apague el equipo al momento de encenderlo empezará con el proceso de respaldo, realizará los respaldos los fines de semana con un tiempo de conservación de 1 mes y se realiza la limpieza después de terminar el respaldo, el archivo de respaldos tendrá un cifrado AES256 con el fin de seguridad de información.

Imagen 43. Crear Plan. Recuperado de: Software Acronis, 20/05/2022.

Ejecutando el plan de respaldo

Una vez que el plan de respaldo fue creado, aparece la siguiente pantalla (Imagen 44 Menú del plan)

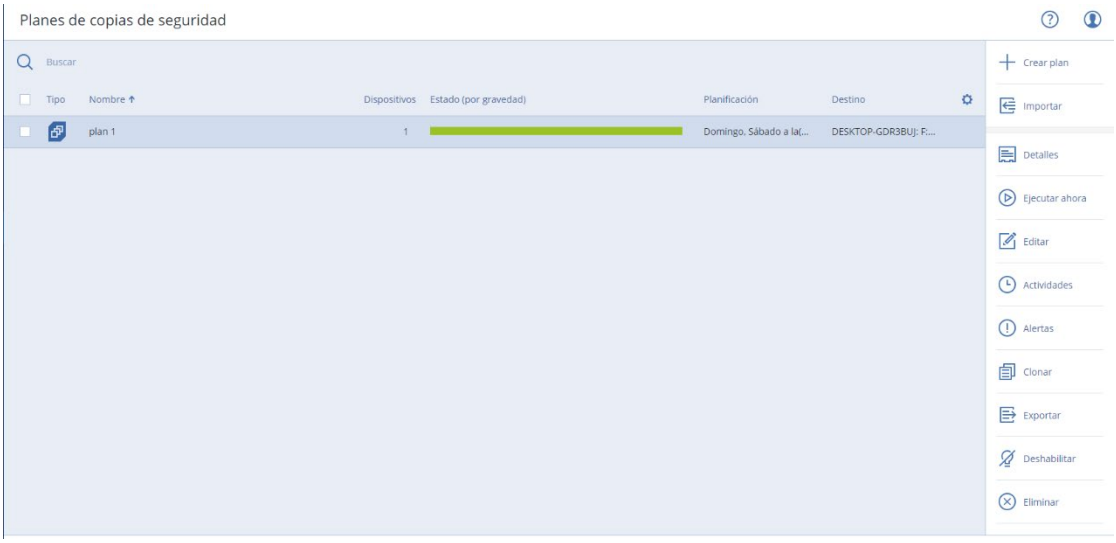

Imagen 44. Menú del plan. Recuperado de: Software Acronis, 20/05/2022.

En la pantalla (nombre de la pantalla) muestra el plan creado y el estatus en el que se encuentra, Acronis maneja un semáforo de colores de estatus en el cual verde significa que todo está correcto, amarillo significa que existe alguna incidencia y rojo que significa que algo salió mal.

En el lado derecho aparece una lista de acciones que se pueden ejecutar con el plan de respaldos.

La opción que importa por el momento es la de “Ejecutar ahora” lo que realiza esta opción esforzar la ejecución del plan de respaldos evadiendo la programación que se le configuró al plan y así ejecutando el respaldo de información.

Una vez forzando la ejecución del plan de respaldos la barra de estado aparecerá en color azul, lo que nos indica que el respaldo está en ejecución (Imagen 45. Estatus del plan).

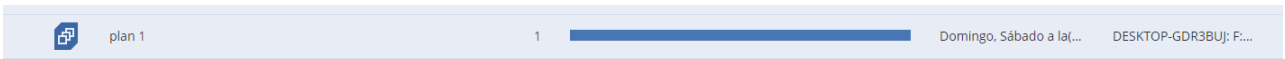

Imagen 45. Estatus del plan. Recuperado de: Software Acronis, 20/05/2022.

Al dar clic en la barra de estatus, mostrara un mensaje que menciona el estado del plan (Imagen 46. Estatus detallado del plan.)

Imagen 46. Estatus detallado del plan. Recuperado de: Software Acronis, 20/05/2022.

Al dar clic al mensaje “En ejecución” mostrara el estatus de los equipos que se están respaldando y el porcentaje completo que lleva el proceso como lo muestra el siguiente mensaje (Imagen 47. Estatus del cliente.).

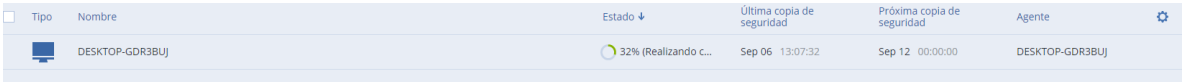

Imagen 47. Estatus del cliente. Recuperado de: Software Acronis, 20/05/2022.

De esta forma se ejecuta el plan de respaldos con el fin de forzar un respaldo desde la consola de Acronis.

Recuperando la información

Acronis contiene 3 métodos para recuperar la información de un cliente.

- Recuperación de información mediante el cliente.
- Recuperación de información mediante los archivos del NAS
- Virtualizar el respaldo.

Solamente se utilizarán las primeras dos opciones, ya que para virtualizar el respaldo es necesario contar con una base sólida sobre el tema de virtualización y de un servidor en especial.

Una vez que se tenga el plan autónomo de respaldo y los agentes instalados, en la consola de Acronis ubicamos la sección de dispositivos y se selecciona la opción

“Equipos con agentes” (Imagen 48. Equipos con agentes.), mostrará los equipos que tienen el agente instalado y la última fecha en la que se realizó el respaldo.

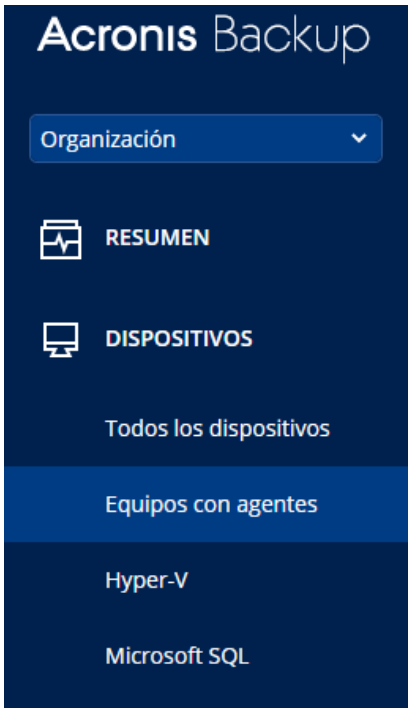

Imagen 48. Equipos con agentes. Recuperado de: Software Acronis, 20/05/2022.

Una vez realizado lo anterior, se selecciona el equipo que se necesita restaurar la información y dar clic en la opción “Restaurar” (Imagen 49. Restaurar

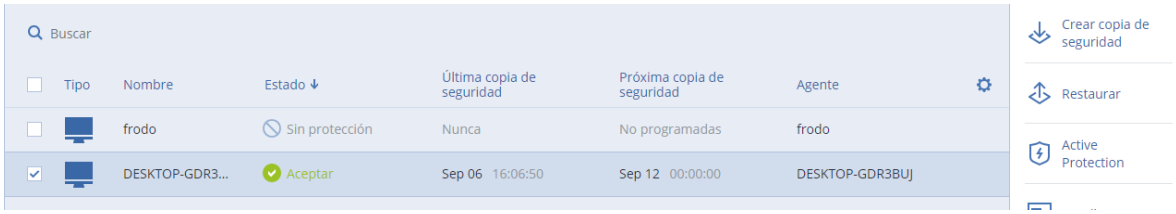

Imagen.)

Imagen 49. Restaurar imagen. Recuperado de: Software Acronis, 20/05/2022.

Al dar clic en la opción mencionada, aparecerá los respaldos incrementales que se realizan en el equipo de cómputo con el fin de reestablecer la información de una fecha en específico (Imagen 50. Respaldos Realizados).

La fecha que arroja el sistema de Acronis empieza desde la primera ejecución del plan de respaldos hasta la fecha, incluso si se ejecutó el plan de respaldos antes de la fecha programada o se ejecutó dos veces al día el plan de respaldo Acronis muestra los respaldos incrementales realizados y la opción para recuperar o ejecutar la imagen del equipo respaldado en una Virtual Machine (Máquina Virtual).

Imagen 50. Respaldos realizados. Recuperado de: Software Acronis, 20/05/2022.

Al dar clic en la opción Recuperar dará las opciones de que es lo que queremos recuperar como se ve en la siguiente pantalla. (Imagen 51. Opciones de recuperación)

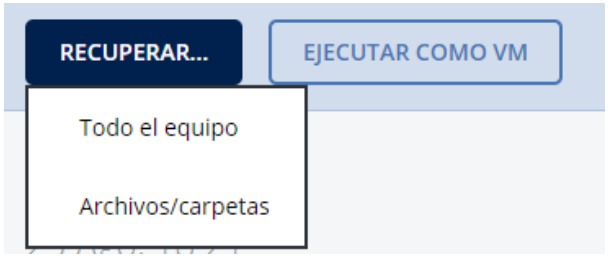

Imagen 51. Opciones de recuperación. Recuperado de: Software Acronis, 20/05/2022.

Recuperación de información de todo el equipo

En la recuperación de todo el equipo, Acronis lo que realiza es crear una imagen con extensión ".tibx", esta extensión es única en Acronis y se empezó implementar desde la versión 12 de Acronis.

Después de dar clic en la opción de recuperación del equipo aparecerá la siguiente pantalla (Imagen 52. Recuperación detallada.)

Imagen 52. Recuperación detallada. Recuperado de: Software Acronis, 20/05/2022.

Para realizar una copia exacta del equipo respaldado se necesita asignar dónde se realizará la clonación del respaldo en los discos duros, por lo tanto, se selecciona la opción de asignación de discos (Imagen 53. Clonación de Disco Duro).

Imagen 53. Clonación de Disco Duro. Recuperado de: Software Acronis, 20/05/2022.

En esta opción se seleccionará el destino de los discos duros que se tiene respaldados del agente, por lo tanto, es necesario que en la consola se tenga conectado los discos duros asignados para realizar el respaldo completo del equipo.

En este caso solamente se realiza la simulación de la recuperación de la información ya que es necesario contar con los discos conectados, en este caso dos discos duros para que la recuperación se realice por completo, por lo tanto, en la parte superior derecha, se encuentra una opción activable llamada “Cambiar a asignación de volúmenes”. Esta opción lo que permite es clonar exactamente los volúmenes al destino que se indique y aparecerá el siguiente menú (Imagen 54. Asignación de Volumen.).

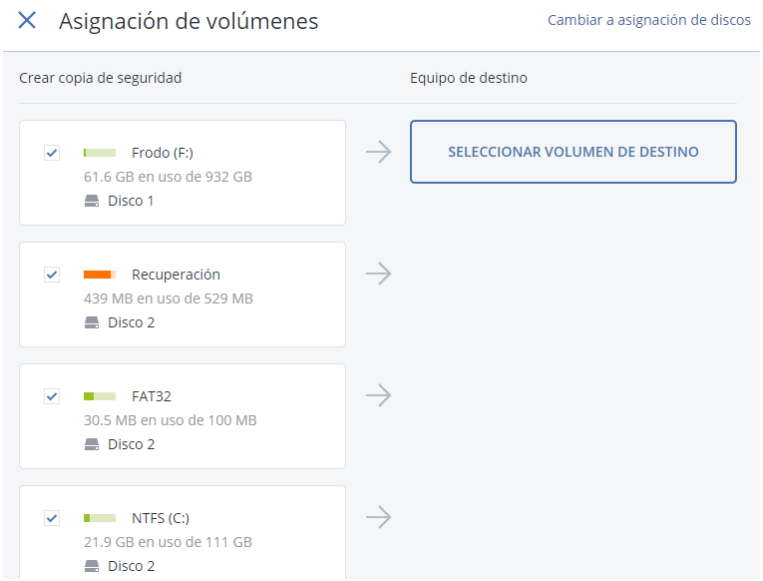

Imagen 54. Asignación de volumen. Recuperado de: Software Acronis, 20/05/2022.

Se selecciona el destino donde se guardará el respaldo del volumen 1 del equipo de cómputo, al dar clic mostrará una pantalla en los diferentes dispositivos de almacenamiento que se puede almacenar (Imagen 55. Selección de volumen), en este caso como el respaldo se está realizando dentro de la misma laptop y no en un NAS, se visualizará cualquier dispositivo de almacenamiento que tiene conectado el equipo, por lo tanto, se conectó un disco duro externo para realizar este ejemplo a nivel gráfico, el disco duro externo está asignado en la unidad D del equipo por lo tanto será el dispositivo de almacenamiento que se seleccionará para realizar la recuperación.

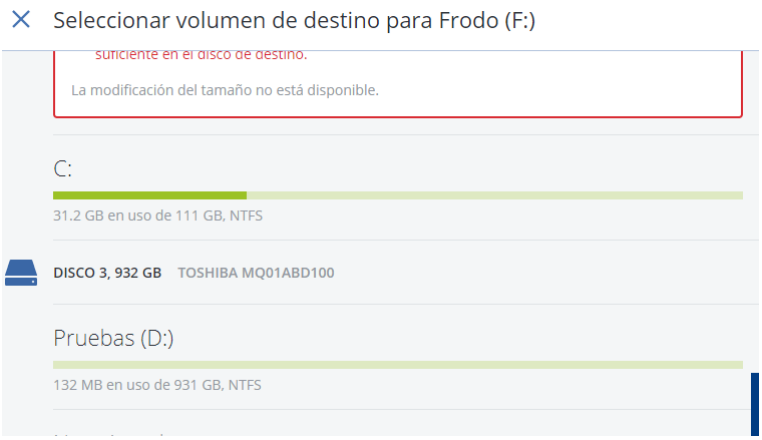

Imagen 55. Selección de volumen. Recuperado de: Software Acronis, 20/05/2022.

Una vez realizado la asignación / selección de los discos duros y sus particiones, se da clic en el botón de finalizar y se ejecuta la recuperación (Imagen 56. Iniciar Recuperación.).

Imagen 56. Iniciar Recuperación. Recuperado de: Software Acronis, 20/05/2022.

Una vez realizada esta operación los discos duros están listos para ser conectados a un equipo de cómputo y mostrar la misma configuración e información del respaldo realizado.

Recuperación de información de Archivos/Carpetas

La recuperación de información de Archivos/Carpetas consiste en realizar una restauración en un solo archivo o simplemente extraer una información específica. Al dar clic en la opción mencionada mostrara las carpetas del respaldo seleccionado (Imagen 57. Selección de Archivos).

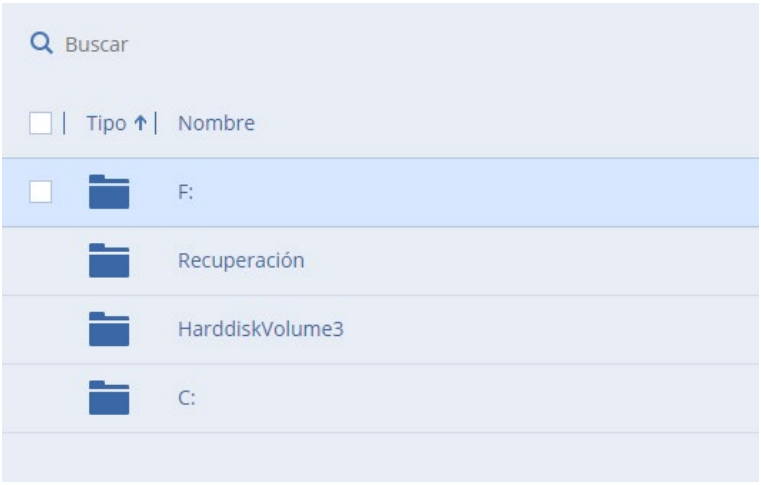

Imagen 57. Selección de archivos. Recuperado de: Software Acronis, 20/05/2022.

Una vez seleccionada los archivos y carpetas a recuperar, Acronis da dos opciones de recuperación.

- Recuperar
- Descargar.

Recuperar

En la opción “Recuperar” empieza con el proceso “recuperación en la ubicación original” donde se encuentra la información o en una “ubicación en específico”, como es necesario sacar el respaldo fuera del NAS, se selecciona la opción “Ubicación Personalizada” y se da clic en “Examinar…” para poder especificar en donde se desea guardar (Imagen 58 Ubicación Personalizada.).

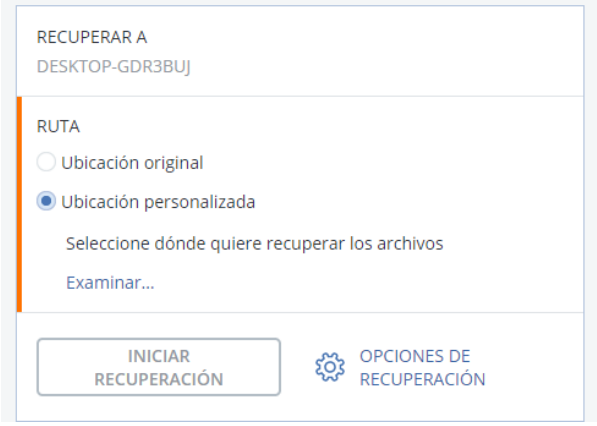

Imagen 58. Ubicación personalizada. Recuperado de: Software Acronis, 20/05/2022.

Una vez seleccionada dicha opción, se puede elegir la ubicación donde se desea guardar el respaldo del equipo (Imagen 59. Selección de ubicación).

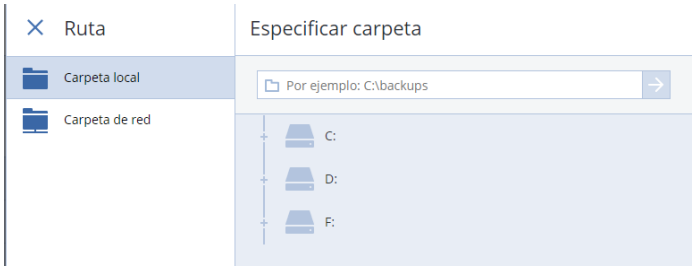

Imagen 59. Selección de ubicación. Recuperado de: Software Acronis, 20/05/2022.

Una vez seleccionado la ubicación y que información se desea recuperar, en la consola muestra el estatus de la recuperación (Imagen 60. Detalles de la actividad).

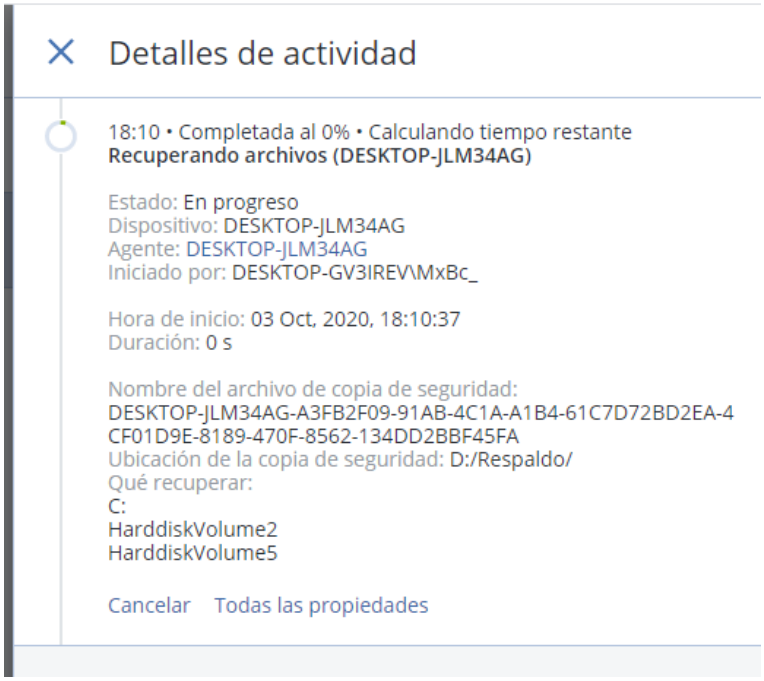

Imagen 60. Detalles de la actividad. Recuperado de: Software Acronis, 20/05/2022.

Cuando termina el proceso de recuperación, en el destinatario aparece una copia exacta de la información respaldada como se muestra en la siguiente pantalla (Imagen 61. Respaldo realizado).

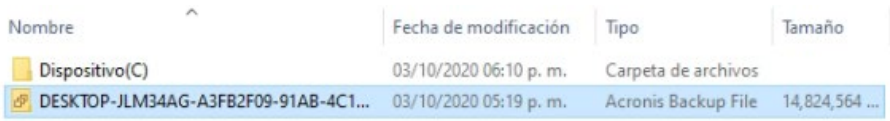

Imagen 61. Respaldo realizado. Recuperado de: Software Acronis, 20/05/2022.

Descargar

En la opción seleccionada, descarga todo el respaldo de la información en un solo archivo comprimido.

Para que la función de descargar se ejecute, al seleccionar las carpetas que se restauran se da clic en la opción descargar (Imagen 62. Selección de Carpetas.).

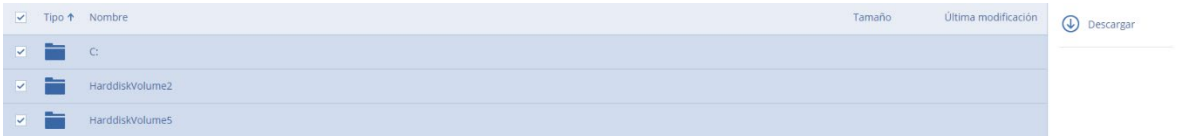

Imagen 62. Selección de carpetas. Recuperado de: Software Acronis, 20/05/2022.

Una vez realizado el navegador que se esté ejecutando, descargará el respaldo completo del cliente seleccionado. (Imagen 63. Descarga de respaldo)

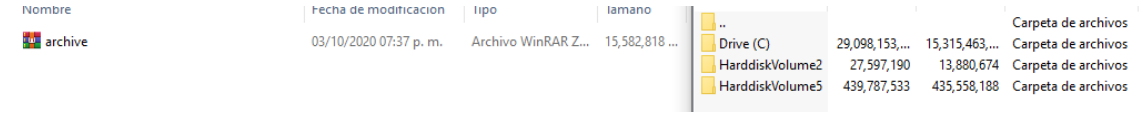

Imagen 63. Descarga de respaldo. Recuperado de: Software Acronis, 20/05/2022.

¿Existen más maneras de recuperar la información?

En algunas nuevas versiones de Acronis es más probable que existan diferentes formas de recuperar la información, se mostraron 2 formas diferentes de recuperar un respaldo con el sistema de Acronis, recordando que es de suma importancia recuperar los archivos “Importantes” ya sean documentos, multimedia, datos personales, etcétera. De las 2 formas que se explicaron se puede realizar una recuperación exitosa y así llevar un correcto control de respaldos de información para los usuarios finales.

Conclusiones

El correcto control de respaldo de información es una medida que se debe de tomar en cuenta en un área de sistemas, debido a que pueden existir diferentes fallas ya sean mediante Hardware y Software en los equipos de cómputo. Se debe de tener claramente desde cómo se implementará el sistema, hasta que componente es el correcto para que no exista falla alguna.

Cabe de destacar que esta implementación fue creada con una infraestructura limitada, no cabe duda de que en otras entidades tengan un plan de respaldo superior al que se mostró en esta tesis, cabe de destacar que en este caso práctico sin importar la infraestructura que este implementada se muestra como implementar el sistema de Acronis y configurarlo correctamente, esta configuración requirió meses optimizarla, ya que no es fácil llegar a esta configuración sin tener una capacitación de Acronis, tampoco es fácil llegar a esta configuración con los manuales que ofrece el proveedor. Recordando que en el mundo de la informática es importante tener el conocimiento actual de todos los componentes informáticos y de igual forma tener la capacidad de que todo sea óptimo y autónomo, para que simplemente se administre.

Por lo tanto, este trabajo de investigación se enfocó para todos los informáticos que no cuentan con la información correcta y la experiencia para implementar un plan de respaldos, también a los estudiantes que no tienen noción de lo que espera en el área de sistemas y puedan conocer una de las actividades más importantes que deben de manejar a la perfección.

Para concluir, al tener el conocimiento previo para poder llevar un correcto control de respaldos de información, junto con los elementos necesarios, podrán realizar una implementación correcta y tener un control correcto de un sistema de respaldos de información, para proteger los datos de ataques informáticos o incidentes externos ya que la información es parte fundamental en cualquier entidad, es un honor compartir este conocimiento de cómo tener un correcto control

de respaldos de información que ha dado resultados satisfactorios para la seguridad de la información de una empresa.

Fuentes de Información

Libros

Areitio Bertolín Javier. (2008). SEGURIDAD DE LA INFORMACIÓN. Redes, Informática y Sistemas de Información. España: Ediciones Paraninfo, S.A.

García Javier. (2003). Fundamentos y Estructura de Computadores. España: S.A. EDICIONES PARANINFO.

González Castellanos Edgardo. (2010). La Computadora Personal y sus conceptos básicos. Estados Unidos de América y Puerto Rico: Primera Edición 2010.

Hernández Sampieri, Roberto. (2001). Metodología de la Investigación. México, D.F: McGraw-Hill.

Huidobro Moya José Manuel. (2014). Telecomunicaciones Tecnologías, Redes y Servicios. Madrid: Ra-Ma S.A. Editorial y Publicaciones.

Katz Ruiz Matías. (2013). Redes y seguridad. España: Marcombo.

Quiroga Patricia. (2010). Arquitectura de Computadoras. España: Alfaomega.

Real Academia Española. (2017). Diccionario de la lengua española (23.a ed.). Madrid, España: Autor.

Terán Pérez David Moisés. (2018). Administración y Seguridad en redes de computadoras. España: Alfaomega.

Vázquez Gómez Juan Bernardo. (2012). FUNDAMENTOS DE LA ARQUITECTURA COMPUTACIONAL. En Arquitectura de Computadoras 1(110). Estado de México: RED TERCER MILENIO S.C.

Valentín López, Gema María. (2016). Grabación De Datos. España: RA-MA S.A. Editorial y Publicaciones.

Páginas Web.

Amazon Web Services. (2019). Almacenamiento en la nube. 15/12/2019, de amazon.com Sitio web: https://aws.amazon.com/es/what-is-cloud-storage/DEFINICION DE RED LIBRO

Armando Moisés Bernal Kaiser, Mireya López Escobar. (2012). Apuntes Digitales Plan 2012. 15/12/2019, de fcasua.contad.unam.mx Sitio web: http://fcasua.contad.unam.mx/apuntes/interiores/docs/2012/informatica/1/1169.pdf

Andrew S. Tanenbaum, David J. Wetherall. (2011). Redes de computadoras. Atlacomulco 500-5o. piso Col. Industrial Atoto 53519, Naucalpan de Juárez, Estado de México: PEARSON.

Acronis. (2020). Comprar Acronis Cyber Protect. 05/02/2020, de Acronis Sitio web: https://www.acronis.com/es-mx/cloud/storage/purchasing/Precios de AWS

Amazon. (2020). Precios de Amazon S3. 05/02/2020, de Amazon Sitio web: https://aws.amazon.com/es/s3/pricing/

BackBlaze. (2020). Datos y estadísticas del disco duro. 05/02/2020, de backblaze.com Sitio web: https://www.backblaze.com/b2/hard-drive-test-data.html

Chiavenato Idalberto. (2006). Introducción a la Teoría General de la Administración. México: McGraw-Hill Interamericana.

EcuRed. (2015). Ataque informático. 05/02/2020, de EcuRed Sitio web: https://www.ecured.cu/Ataque_inform%C3%A1tico

EcuRed. (2015). Protocolos de red. 20/01/2020, de ecured Sitio web: https://www.ecured.cu/Protocolos_de_redPrecio de Acronis tabla 3.2

Facultad de Medicina Veterinaria y Zootecnia. (2005). Dispositivos de almacenamiento y transportación de datos. 05/02/2020, de fmvz.unam.mx Sitio

web:
http://www.fmvz.unam.mx/fmvz/secretarias/tecnologia/manuales/m_almacena.pdf

Hewlett Packard. (2018). ¿QUÉ ES EL ALMACENAMIENTO DE DATOS? 05/02/2020, de hpe.com Sitio web: https://www.hpe.com/mx/es/what-is/data-storage.html

Ivan Bravo. (20117). ¿Qué es un equipo de cómputo y sus características? 05/02/2020, de reparando.com Sitio web: https://reparando.com.mx/que-es-un-equipo-de-computo-y-sus-caracteristicas/

James Griffiths. (2016). EE.UU. todavía usa floppy disks… ¡en su programa nuclear! 05/06/2020, de cnnespañol Sitio web: https://cnnespanol.cnn.com/2016/05/26/ee-uu-todavia-usa-floppy-disks-en-su-programa-nuclear/

Juan Lanchares Dávila. (2 012). Apuntes de Estructura de Computadores. 24/11/2019, de Universidad Complutense Madrid Sitio web: http://www.dacya.ucm.es/lanchares/documentos/2.9.5%20Apuntes%20de%20Estructura%20de%20Computadores.pdf

Manuel Santos. (2018). Estos son los discos duros con mayor capacidad que podemos comprar. 05/02/2020, de hardzone.es Sitio web: https://hardzone.es/2018/07/28/discos-duros-mayor-capacidad/

Malwarebytes. (2020). Ransomware. 05/02/2020, de malwarebytes.com Sitio web: https://es.malwarebytes.com/ransomware/

Malwarebytes. (2020). Spyware. 05/02/2020, de malwarebytes.com Sitio web: https://es.malwarebytes.com/spyware/

Malwarebytes. (2020). Suplantación de identidad (phishing). 2020, de malwarebytes.com Sitio web: https://es.malwarebytes.com/phishing/

Raúl Álvarez. (2019). China ya tiene 219 de los 500 supercomputadores más potentes del mundo, mientras EEUU domina el top 10. 05/02/2020, de xataka.com Sitio web: https://www.xataka.com/ordenadores/china-tiene-219-500-supercomputadores-potentes-mundo-eeuu-domina-top-10

Riquelme, R. (2019, 10 abril). Pérdida de datos le cuesta a una empresa en México más de 1 millón de dólares: DELL EMC. El Economista. https://www.eleconomista.com.mx/tecnologia/Perdida-de-datos-le-cuesta-a-una-empresa-en-Mexico-mas-de-1-millon-de-dolares-DELL-EMC-20190410-0079.html

Rosaura Arteaga Rojas - Sonia Luz Pardo López. (2012). Licenciatura en Administración. 24/11/2019, de Facultad de Contaduría Y Administración. Sitio web: http://fcasua.contad.unam.mx/apuntes/interiores/docs/2012/administracion/4/1425.pdf

Red Hat. (2019). El concepto de almacenamientos de datos. 01/12/2019, de redhat.com Sitio web: https://www.redhat.com/es/topics/data-storage

Salvador Meza Badillo. (2005). Telecomunicaciones I. 15/01/2020, de Sistema Universidad Abierta y Educación a Distancia Sitio web: http://fcasua.contad.unam.mx/apuntes/interiores/docs/2005/informatica/4/1467.pdf

SEAGATE. (2019). ¿Qué es NAS (almacenamiento conectado en red) y Por qué el NAS es importante para una pequeña empresa? 15/12/2019, de seagate.com Sitio web: https://www.seagate.com/la/es/tech-insights/what-is-nas-master-ti/

Universidad Nacional Experimental Simón Rodríguez. (2004). Estructura y Topologías de las Redes Informáticas. 15/01/2020, de edesinformaticasipodd.blogspot.com Sitio web: http://redesinformaticasipodd.blogspot.com/2014/11/3-estructura-y-topologias-de-las-redes.html

Universidad de Valencia. (2016). LAN, WAN, MAN y otras redes. 15/01/2020, de Universidad de Valencia Sitio web: https://www.uv.es/uvweb/master-ingenieria-telecomunicacion/es/blog/lan-wan-man-otras-redes-1285954593702/GasetaRecerca.html?id=1285959494096

Universidad Internacional de Valencia. (2018). ¿Qué es la seguridad informática y cómo puede ayudarme? 05/02/2020, de Universidad Internacional de Valencia Sitio web: https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/