

▪ Gradu Amaierako Lana ▪

Konputagailuen Ingeniaritza

SEGURTASUN KOPIAK BURUTZEN DITUEN AZPIEGITURA  
BAT MARTXAN JARTZEA

---

Egilea

Ion Molla Mena

Zuzendaria

Jose A. Pascual

Enpresako Zuzendaria

Vincent Seres

*2019 - Iraila*



# Laburpena

---

Zer gertatuko litzateke ordenagailuan gordetzen den informazio guztia (dokumentuak, argazkiak, pasahitzak, posta elektronikoko mezuak etab.) galduko balitz?

Gaur egun, informazioa eta datuak gordetzeko, bai etxean edota enpresetan ere, ordenagailua da erabiltzen den gailu nagusia. Enpresen kasuan, informazioa erritmo altu batean sortzen da, ondorioz, informazioa enpresaren nukleoa bihurtzen da. Hori dela eta, ez dago dudarik, enpresa batean informazioa dela garrantzitsuena eta baliotsua egiten duena.

Datu galera saihesteko, argi dago segurtasun neurriak hartu behar direla sarean, sisteman eta garrantzitsuena, noizbehinka ahazten dena, **segurtasun kopiak** burutzea. Hori guztiarengatik eta dokumentuan zehar azalduko diren argudioengatik, egoitza batean segurtasun kopiak burutzen dituen azpiegitura bat martxan jartzea burutuko da.

Lehenik eta behin, segurtasun kopiei buruzko kontzeptuen analisi teoriko bat egingo da. Ondoren, kontzeptu horiek segurtasun kopiak burutzen dituen programa batean aplikatuko dira. Gaur egun, segurtasun kopiak burutzeko hainbat programa erabili daitezke, hori dela eta, bi programa alderatuko dira, haien abantailak eta desabantailak aipatuz. Azkenik, segurtasun kopien egoera eta informazioa aztertzeke eta eskuratzeko script bat programatuko da, prozesua automatizatzeke.



# Resumen

---

¿Qué pasaría si de repente toda la información que se almacena en el ordenador (documentos, fotografías, contraseñas, mensajes de correo electrónico, etc.) desapareciera?

Hoy en día el ordenador se utiliza como herramienta base de almacenamiento de datos, tanto como para uso personal como para empresas. En el caso de esta última, la información se produce a un ritmo muy acelerado, incluso los datos se han convertido en el núcleo de cualquier empresa. Por lo tanto, no caben dudas de que para una empresa su información es lo más importante y lo que la hace valiosa.

Para evitar la pérdida de datos, ya se sabe qué se debe ser precavido en el funcionamiento de la red y sistemas y algo muy importante que a veces se olvida es realizar **copias de seguridad**. Por todos estos motivos y por alguno más que se irá comentando a lo largo de este documento, se realizará una puesta en marcha de una infraestructura *Backup*.

Para empezar, se realizará un análisis teórico sobre los conceptos de copias de seguridad. Después estos conceptos se aplicarán a una herramienta que realiza copias de seguridad. Actualmente, se pueden utilizar diferentes programas para realizar los *Backups*, por lo tanto, se hará una comparativa de dos herramientas, comentando sus ventajas y desventajas. Por último, se programará un *script* automático para obtener la información y el estado de las copias de seguridad.



# Gaien Aurkibidea

---

<b>LABURPENA.....</b>	<b>2</b>
<b>RESUMEN .....</b>	<b>4</b>
<b>GAIEN AURKIBIDEA .....</b>	<b>6</b>
<b>IRUDI ETA TAULEN ZERRENDA.....</b>	<b>8</b>
<b>HITZ GAKOAK .....</b>	<b>10</b>
<b>AURKEZPENA.....</b>	<b>12</b>
1.1 SARRERA.....	13
1.2 PROIEKTUAREN DESKRIBAPENA.....	14
1.2.1 <i>Enpresa</i> .....	14
1.2.2 <i>Proiektua</i> .....	14
<b>PROIEKTUAREN HELBURUEN DOKUMENTUA .....</b>	<b>18</b>
2.1 PROIEKTUAREN HELBURUEN DOKUMENTUEN ANTOLAKETA .....	19
2.2 PROIEKTUAREN HELBURUAK.....	19
2.3 LAN METODOLOGIA.....	20
2.4 PLANGINTZA.....	21
2.4.1 <i>Atazen deskonposaketa</i> .....	21
2.4.2 <i>Orduen estimazioa eta egutegia</i> .....	23
2.4.3 <i>Gantt diagrama</i> .....	25
2.4.4 <i>Arrisku plana</i> .....	26
2.5 JARRAIPENA ETA KONTROLA.....	27
2.5.1 <i>Desbiderapenen taula eta azterketa</i> .....	27
<b>ERABILITAKO TEKNOLOGIAK .....</b>	<b>30</b>
3. ERABILITAKO TEKNOLOGIAK.....	31
3.1 AURREKARIEN ANALISIA .....	31
3.2 <i>BACKUP</i> AZPIEGITURA BATEN OSAGAIAK .....	34
3.2.1 <i>Proiektuko azpiegituraren osagaiak</i> .....	36
3.3 HARDWARE ETA SOFTWAREA .....	37
3.4 MOTAK .....	40
3.4.1 <i>Segurtasun kopia osoa</i> .....	40
3.4.2 <i>Segurtasun kopia inkrementala</i> .....	41
3.4.3 <i>Segurtasun kopia diferentziala</i> .....	42
3.4.4 <i>Ispiluaren segurtasun kopia</i> .....	42
<b>ANALISIA .....</b>	<b>44</b>
4.1 SEGURTASUN KOPIAK BURUTZEKO PROGRAMEN EZAUGARRIAK .....	45
4.2 <i>SOFTWARE</i> AUKERAKETA .....	46
4.2.1 <i>Funtzionamendua</i> .....	46
4.3 DEDUPLIKAZIOA .....	47
4.3.1 <i>Motak</i> .....	47
4.3.2 <i>Funtzionamendua</i> .....	48
4.3.3 <i>Noiz erabili</i> .....	48
4.4 ERREKUPERAZIO PLANA.....	49
4.4.1 <i>RPO</i> .....	49
4.4.2 <i>RTO</i> .....	50
4.4.3 <i>Nola definitu RTO eta RPO parametroak</i> .....	50
<b>GARAPENA .....</b>	<b>52</b>

5.1	PROBA FASEA .....	53
5.2	FASE FINALA .....	59
5.3	EMAITZEN ANALISIA .....	61
5.4	SCRIPT-EN PROGRAMAZIOA .....	65
5.5	AURRERA ERAMATEKO PROPOSAMENAK.....	71
<b>KONPARAKETA .....</b>		<b>74</b>
6.1	SOFTWAREAREN KONPARAKETA.....	75
6.1.1.	<i>Veeam Backup</i> .....	75
6.1.2.	<i>Arcserve UDP</i> .....	76
6.1.3.	<i>Konparaketa</i> .....	77
	Erabilera.....	77
	Kostua .....	77
	Funtzioak .....	78
<b>ONDORIOAK.....</b>		<b>80</b>
7.1	PROIEKTUAREN ONDORIOAK .....	81
7.2	IKASITAKOAK .....	81
<b>A ERANSKINA – ARCSERVE UDP KONFIGURAZIOA .....</b>		<b>84</b>
	KONTSOLAREN KONEKXIOA .....	84
	NODOEN GEHIKUNTZA .....	84
	AGENTEAREN INSTALAZIOA NODOETAN .....	85
	KOKALEKUA ESPEZIFIKATU.....	85
	DATU BILTEGIA SORTU.....	86
	PLAN BAT SORTU.....	87
	SEGURTASUN KOPIA MANUALA PROGRAMATU .....	89
	SEGURTASUN KOPIEN BERRESKURAPENA .....	89
<b>B ERANSKINA – EMAITZAK .....</b>		<b>94</b>
<b>C ERANSKINA – BILERA AKTAK .....</b>		<b>98</b>
B.1	KONSTITUZIO BILERA .....	98
B.2	LEHENENGO BILERA.....	98
B.3	BIGARREN BILERA .....	99
B.4	HIRUGARREN BILERA .....	99
B.5	LAUGARREN BILERA.....	100
B.6	BOSGARREN BILERA.....	101
B.7	SEIGARREN BILERA .....	101
<b>BIBLIOGRAFIA.....</b>		<b>102</b>



# Irudi eta Taulen zerrenda

---

## IRUDIAK

1.1. IRUDIA. EGOITZEN ESKEMA OROKORRA.....	15
2.1. IRUDIA. HELBURUEN LABURPENA. ....	19
2.2. IRUDIA. LDE DIAGRAMA. ....	21
2.3. IRUDIA. GANTT DIAGRAMA. ....	25
3.1. IRUDIA. TEKNOLOGIEN DENBORA DIAGRAMA.....	31
3.2. IRUDIA. ZINTA AZPIEGITURA. ....	36
3.3. IRUDIA. DISKO AZPIEGITURA. ....	37
3.4. IRUDIA. SEGURTASUN KOPIA OSOAREN FUNTZIONAMENDUA.....	41
3.5. IRUDIA. SEGURTASUN KOPIA INKREMENTALAREN FUNTZIONAMENDUA.....	41
3.6. IRUDIA. SEGURTASUN KOPIA DIFERENTZIALAREN FUNTZIONAMENDUA. ....	42
3.7. IRUDIA. ISPILU SEGURTASUN KOPIAREN FUNTZIONAMENDUA. ....	42
4.1. IRUDIA. ARCSERVE UDPREN FUNTZIONAMENDUA. ....	46
4.2. IRUDIA. DEDUPLIKAZIOAREN FUNTZIONAMENDUA. ....	48
4.3. IRUDIA. RPO ETA RTO KONPARAKETA. ....	49
5.1. IRUDIA. TAMAINA ESTIMAZIOA.....	54
5.2. IRUDIA. PLAN BAT SORTZEKO PROZEDURA. ....	55
5.3. IRUDIA. VMWARE ESXI ZERBITZARI BATEN EGITURA. ....	58
5.4. IRUDIA. SEGURTASUN KOPIEN TAMAINEN ARTEKO KONPARAKETA.....	62
5.5. IRUDIA. TAMAINAREN EBOLUZIOA. ....	63
5.6. IRUDIA. SEGURTASUN KOPIEN DENBOREN ARTEKO KONPARAKETA. ....	63
5.7. IRUDIA. VEEAM-GETJOBS FUNTZIOAREN ADIBIDEA. ....	68
5.8. IRUDIA. POWERBI PROGRAMA BITARTEZ SORTUTAKO AUTOMATIZAZIOA. ....	70
5.9. IRUDIA. DATU BILTEGIA EZ DAGOEN EGOITZA BATEKO SEGURTASUN KOPIAREN PROZESUA. 72	
5.10. IRUDIA. DTC ETA LYO ARTEKO TRAFIKOAREN KONTROLA.....	72
5.11. IRUDIA. EGOITZETAN DATU BILTEGIA DAGOEN SEGURTASUN KOPIAREN PROZESUA. ....	73
A.1. IRUDIA. NODOA GEHITU. ....	85
A.2. IRUDIA. RPS-A GEHITU. ....	86
A.3. IRUDIA. DATU BILTEGIA SORTU. ....	87
A.4. IRUDIA. "DESTINATION" KONFIGURAZIOA. ....	88
A.5. IRUDIA. "SCHEDULE" KONFIGURAZIOA. ....	88
A.6. IRUDIA. "BACKUP RECOVERY" MOTAK. ....	90
A.7. IRUDIA. ARTXIBOEN AUKERAKETA. ....	90
A.8. IRUDIA. MAKINA BIRTUAL BAT BERREZARTZEKO AUKERAK. ....	91

<b>A.9. IRUDIA. MAKINA BIRTUAL BAT BERREZARTZEKO AUKERA AURRERATUAK. ....</b>	<b>92</b>
---	-----------

## TAULAK

<b>2.1. TAULA. ATAZEN ESTIMAZIO DENBORAK. ....</b>	<b>24</b>
<b>2.2. TAULA. ESTIMATUTAKO ETA DEDIKATUTAKO DENBORAREN ARTEKO KONPARAKETA. ....</b>	<b>28</b>
<b>3.1. TAULA. LYO EGOITZAKO ZERBITZARIEN DATUAK. ....</b>	<b>38</b>
<b>3.2. TAULA. SEGURTASUN KOPIEN MOTEN LABURPENA. ....</b>	<b>40</b>
<b>5.1. TAULA. FASE FINALAREN PLANEN EZAUGARRIAK. ....</b>	<b>59</b>
<b>6.1. TAULA. VEEAM BACKUP EZAUGARRIAK. ....</b>	<b>75</b>
<b>6.2. TAULA. ARCSERVE UDP EZAUGARRIAK. ....</b>	<b>76</b>
<b>B.1. TAULA. ZINTAN KOPIATU DIREN BTFISPLYO01 ZERBITZARIAREN EMAITZAK. ....</b>	<b>94</b>
<b>B.2. TAULA. DISKOAN KOPIATU DIREN BTFISPLYO01 ZERBITZARIAREN EMAITZAK. ....</b>	<b>94</b>
<b>B.3. TAULA. BTFISPLYO05 PROBA ZERBITZARIAREN EMAITZAK. ....</b>	<b>95</b>
<b>B.4. TAULA. LYO EGOITZAKO BESTE ZERBITZARIEN EMAITZAK. ....</b>	<b>95</b>
<b>B.5. TAULA. BESTE EGOITZA BATEKO ZERBITZARIEN EMAITZAK. ....</b>	<b>96</b>
<b>B.6. TAULA. BTFISPLYO11 ZERBITZARIAREN BERRESKURATZE DENBORAK. ....</b>	<b>96</b>
<b>B.7. TAULA. BTFISPLYO11 MAKINA BIRTUALAREN BERRESKURATZEA. ....</b>	<b>96</b>

## KODEAK

<b>5.1. KODEA. SQL-QUERYDB FUNTZIOAREN DEFINIZIOA. ....</b>	<b>65</b>
<b>5.2. KODEA. DATU BASEAREN KONEXIOA. ....</b>	<b>66</b>
<b>5.3. KODEA. SQL KONTSULTA. ....</b>	<b>67</b>
<b>5.4. KODEA. INFORMAZIOA DAGOKION HASH-TAULAN TXERTATZEA. ....</b>	<b>68</b>
<b>5.5. KODEA. DATU BASEAREN INFORMAZIOA EGIAZTATU. ....</b>	<b>69</b>

# Hitz gakoak

---

- **Backup:** Segurtasun kopia egitea sistema baten informazioa, baliabide erauzkor batean gordetzeari (toki seguru batean gorde ahal izateko) deritzo.
- **MPLS** (*MultiProtocol Label Switching*): Konputagailu sareen eta telekomunikazioen munduan, datuak garraiatzeko mekanismo bat da.
- **DEV** (*Development*): Proiektua garatzeko eta aldaketak egiteko ingurunea.
- **QA** (*Quality Assurance*): DEV ingurunean burutu diren proiektuak eta garapenak probatzeko ingurunea.
- **PROD** (*Production*): Proiektua martxan jartzeko ingurunea.
- **D2D** (*Disk to Disk*): Segurtasun kopia diskoan burutzea.
- **RAID** (*Redundant Array of Independent Disks*): Batera funtzionatzen duten disko gogorren multzoren biltegitze sistema da.
- **LTO** (*Linear Tape-Open*): Datuak biltegitzeko zinta mota.
- **DTC** (*Data center*)
- **RTO** (*Recovery Time Objective*): Hondamendi baten ondoren, sistema batek errekuaratzeko behar duen denbora da.
- **RPO** (*Recovery Point Objective*): Hondamendi bat gertatzen den momentutik gal daitezkeen datu maximora iritsi baino lehenagoko denbora tartea definitzen du.
- **SLA** (*Service Level Agreement*): Zerbitzua eskaintzen duen ekoizlearen eta bezeroaren arteko kalitatezko zerbitzua bermatzen duen hitzarmena da.
- **IT** (*Information technology*)
- **RPS** (*Recovery Point Server*): Segurtasun kopiak gordetzeko zerbitzaria.
- **RP** (*Recovery Point*): Segurtasun kopia bat berreskuratzeko puntua.
- **DC** (*Domain Controller*)
- **AD** (*Active Directory*)
- **VMware ESXi:** Birtualizazio plataforma bat da.



*1*



Aurkezpena

## 1.1 Sarrera

---

Gaur egun, zibersegurtasunari edota informatikaren segurtasunari buruz hitz egiten badugu, seguru nago zenbait kontzeptu burura etortzen zaizkigula, hala nola, antibirusak, suhesiak, hackerrak, erasoak, etab. Kontzeptu eta termino guzti hauen artean segurtasun kopiak edo *Backup*-ak (Ingeleseko termino ezaguna Interneten) agertzen dira, hauek oso garrantzitsuak baitira segurtasunaren arloan.

Segurtasun kopia edo babes kopia egitea sistema baten informazioa, baliabide erauzkor batean gordetzeari (toki seguru batean gorde ahal izateko) deritzo. Galera posibleen aurrean, sistema informatiko batek berreskuratze-kapazitatea izatea da kopien helburu nagusia, batez ere enpresentzat oso garrantzitsua den arazoa. Egunero agertzen dira enpresaren datuak eta artxiboak arriskuan jartzen dituzten mehatxuak edo arazoak. Arazo horiek, ustekabeko datuen ezabaketa izan daitezke, hau da, gizaki baten akatsa edota *ransomware* eraso bat ere. Kasu horietan, erasotzaileak *malware* baten bitartez datuak zifratzen ditu eta ondoren dirua eskatzen du datuak desblokeatzeko. Arazo horiek saihesteko oso garrantzitsua da *Backup* azpiegitura egoki eta eraginkor bat izatea enpresa babesteko.

Badira enpresen zenbait kasu, segurtasun-istripu baten ondoren sistemaren aurreko egoera berreskuratzeko aukera ez izateagatik desagertu direla, enpresentzat informazioa baita baliotsua egiten duena. Arazo hau ez da soilik enpresaren arloan gertatzen, izan ere, gailu pertsonaletan dauden datuen galera ere arriskutsua izan daiteke. Baliteke oraingoan ez izatea informazio kritikoa, baina argi dago ez zaiola inori gustatzen bere oroitzenak galtzea (argazkiak, bideoak etab.). Azken finean, ez zara kontziente segurtasun kopiek duten garrantzia istripu edo hondamendi bat gertatu arte.

Segurtasun kopiei esker, edozein motako informazioa gorde daiteke (datu base zehatz batena, posta elektronikarena ...) baliabide desberdinetan (CD-ROM grabagarria, zinta...). Metodo eta teknika berriak sortzen ari dira, hauen eraginkortasuna eta erabilgarritasuna handituz. Geroz eta informazio gehiago gorde, ondoren informazio gehiago berreskuratzeko aukera izango duzu, sistema informatikoa, galerarik gertatu ez balitz bezala utziz. Beti ere, oso garrantzitsua da segurtasun kopien egoera konprobatzea, ondoren gordetako informazioa berreskuratzerako orduan, ez duelako ezertarako balio segurtasun kopiak burutzea ondoren ezingo bada hori berreskuratu.

Argi dago segurtasun kopien garrantzia handia dela gaur egun, beraz, kontuan eduki behar den prozesua da. Hori dela eta, proiektu honetan zehar, egoitza desberdinetan dauden sistemak babesteko segurtasun kopien plana nola burutu eta programatu den azalduko da. Programa bati esker, planifikatutako plana aurrera eraman da, pauso guztiak proiektuan islatuz. Bukatzeko, segurtasun kopien egoera aztertzeko eta informazioa lortzeko prozesu automatikoa programatu da *script* baten bitartez.

Datu bitxi bezala, esan beharra dago 2010etik aurrera, urtero, Martxoaren 31ean, segurtasun kopien egun mundiala ospatzen dela.

## 1.2 Proiektuaren deskribapena

---

Proiektuaren deskribapena hobeto ulertzeko, lehenik eta behin proiektua garatu den enpresaren helburuak eta funtzioak azalduko dira.

### 1.2.1 Enpresa

*Ibermática, Informazioaren eta komunikazioaren teknologiak* (IKT) eskaintzen dituen Espainiako enpresa bat da. 1973. urtean sortu zen eta egoitza Donostian du. Bere arloak honakoak dira:

- Informazio eta komunikazioen teknologiaren aholkularitza.
- Ekipamendu eta azpiegitura.
- Informazio-sistemen integrazioa.
- *Outsourcing*.
- Kudeaketa enpresarialaren konponbidea.

Enpresa, talde ezberdinez osatuta dago, arloaren arabera antolatuta. Nik lan egin dudan taldearen helburua, zenbait bezerori administrazio eta monitorizazio zerbitzua ematea da. Kasu honetan, niri horietako bezero bat tokatu zait, beraz, proiektu hau beste enpresa baten onurarako burutua izan da. Proiektuan agertzen diren datu batzuk aldatuak izango dira informazio konfidentziala dela eta.

Enpresa honek egoitza desberdinak ditu munduan zehar. Egoitza bakoitza azpiegitura desberdinez osatuta dago, hau da, ezaugarri desberdinekin. Lan hau, LYO izeneko egoitzan dagoen azpiegiturari aplikatuko zaio.

### 1.2.2 Proiektua

Aurreko kapituluan aipatu den bezala, proiektu hau segurtasun kopiak burutzen dituen azpiegitura baten martxan jartzean datza.

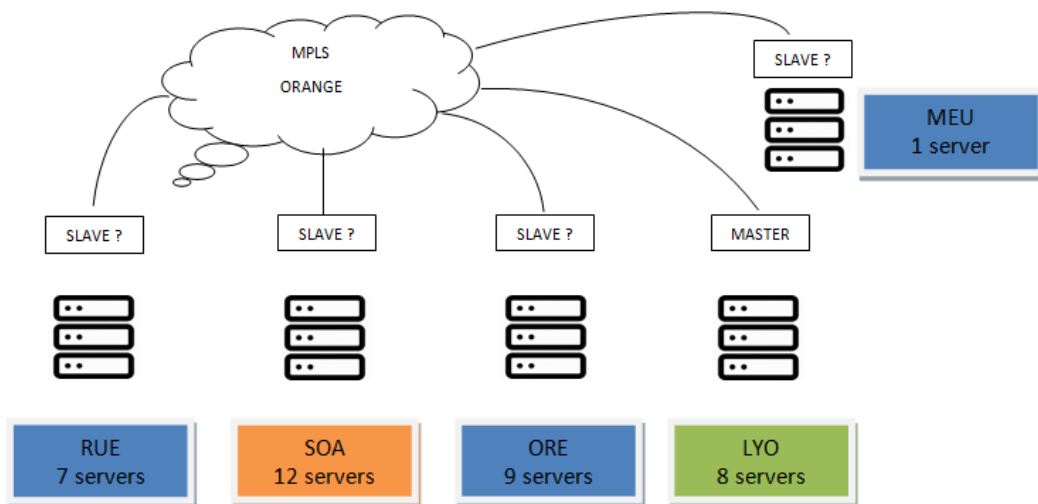
*Arcserve UDP*-n oinarrituz, segurtasun kopiak burutzen dituen programa, azpiegitura berri bat sortuko da LYO egoitzan, zerbitzari batek, *Backup masterra* deritzona, besteekiko kontrol guztia izanik. Gaur egun, egoitza honetako beste zerbitzari batek badu segurtasun kopiak burutzen dituen programa bat instalatuta, zehazki, *Arcserve Backup*. Lehenengoak, kopiak diskoan burutuko ditu, bigarrenak aldiz, zintan egiten ditu. Hori dela eta, lehengo fasean, gaur egun, egiten den prozesuaren hobekuntza egingo da biltegitratze gailua eta planifikazioa aldatuz, baina fase honetan soilik proba zerbitzari bati aplikatuko zaio. Bigarren fasean, egoitza guztiari aplikatuko zaio, zerbitzari multzo bakoitzari plan bat ezarriz. Azkenik, hobekuntza moduan bi metodoak nahastuko dira eraginkortasuna handituz.

Momentuz, zerbitzari bakar bat ezartzen da, *Backup Master* izango dena. Programa honen kontsolaren bitartez, *Backup Master* zerbitzariak beste zerbitzari guztien kontrola izango du. Agente bat instalatuko da zerbitzari guztietan, kontsolaren eta zerbitzari bakoitzaren arteko konexioa ezartzeko. Sistema guztien kontrola kontsolatik egingo da, hau da, urruneko konexio baten bitartez. Windows eta Linux sistema eragileak dituzten sistemak soilik egongo dira nahiz eta zerbitzari fisikoak edo birtualak izan.

Hasieran, funtzionamendu egokia bermatu bitartean, babestuko diren sistemak LYO egoitzan dauden zerbitzariak izango dira. Funtzionamendua bermatuta dagoenean, beste egoitza batzuetako zerbitzariekin probatuko da. Egoitza berean dauden zerbitzarien arteko konexioa LAN bidez izango da, beste egoitza batzuetan dauden zerbitzarien arteko konexioa aldiz, *MultiProtocol Label Switching* (MPLS) bidez. Protokolo hau, datuak garraiatzeko mekanismo bat da.

1.1 irudian azaltzen da egoitzen eskema orokor bat:

- *Backup Masterra* kokatzen den egoitza berdez agertzen da, bertan *Arcserve UDP* programa erabiliko da.
- Laranja agertzen den egoitzan, *Networker* programa erabiltzen da.
- Urdinez agertzen diren egoitzetan, *Arcserve Backup* programa erabiltzen da.



1.1. irudia. Egoitzen eskema orokorra.



Hauek izango dira bete beharreko baldintza minimoak, egoitz zehatz hauetan:

- **LYO:** Lehenetasun handiko azpiegitura eta fitxategi edo aplikazio zerbitzarientzat eguneroko segurtasun kopia burutu asteburua izan ezik. Lehenetasun ertaina eta baxua duten azpiegitura eta fitxategi edo aplikazio zerbitzarientzat astero segurtasun kopia burutu. Bi urteko erretentzioarekin<sup>1</sup>.
- **Beste egoitzak** : Lehenetasun altuko azpiegitura eta fitxategi edo aplikazio zerbitzarientzat eguneroko segurtasun kopia burutu asteburua izan ezik. Bi urteko erretentzioarekin.

Segurtasun kopiak burutzen dituzten bi programen (*Arcserve UDP* eta *Veeam*) analisi eta konparaketa bat egingo da, gaur egun, merkatuan segurtasun kopiak burutzeko indar gehien duten programak bait dira.

Zerbitzarian ere *script* desberdinak programatuko dira:

- a. Segurtasun kopien egoera eta informazioa gordetzen duen prozesu automatikoa programatuko da.
- b. Segurtasun kopien kontrol automatikoa programatuko da. Honi esker, finkatutako periodo batean exekutatu dira nahi diren segurtasun kopiak.

---

<sup>1</sup> Enpresa batek zehazten duen politika bat da, datu edo dokumentu mota desberdinei epe bat esleitzen zaie sortu diren datatik. Data hori pasata gordetako informazio hori ezabatzeko aukera dago, lehenago ez.



# 2



## Proiektuaren Helburuen Dokumentua

## 2.1 Proiektuaren Helburuen Dokumentuen antolaketa

---

Atal honetan proiektuaren helburuak eta proiektua aurrera eramateko plangintza azalduko dira.

Lehenik eta behin, proiektuan gauzatu behar diren helburuak eta hauek lortzeko erabili den lan metodologia azalduko da. Behin helburuak definituta daudela, hauek lortzeko definitu diren atazak azalduko dira, noiz burutuko diren eta haien dedikazioaren estimazio bat definituz.

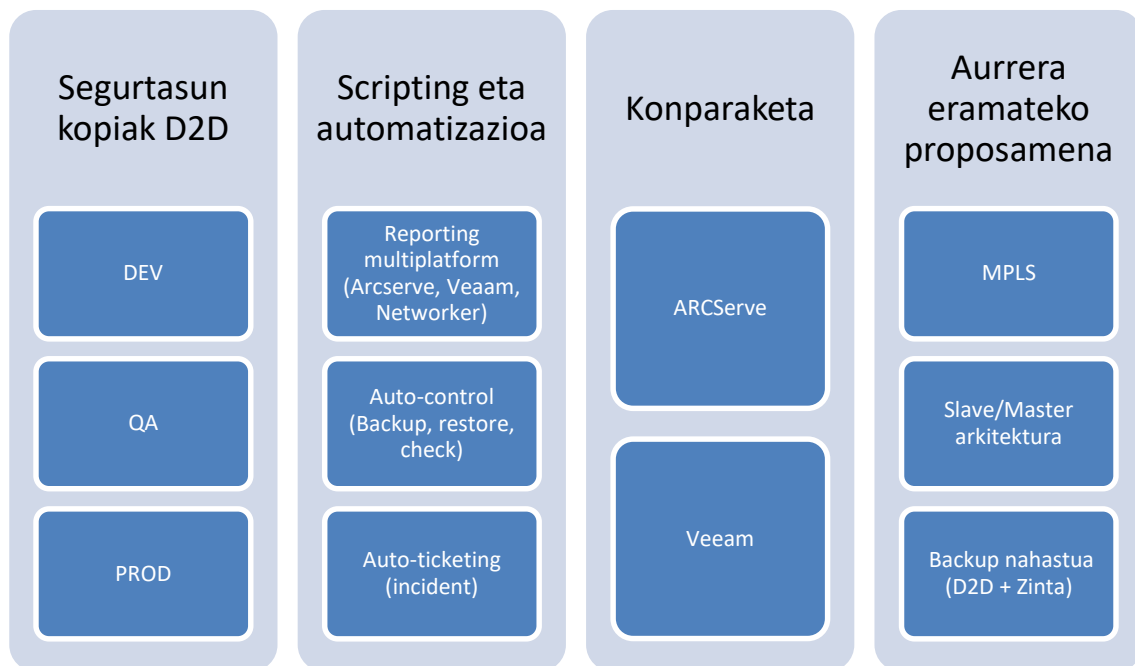
Ondoren, lanaren kontrol eta jarraipen bat burutu da, atazetan estimatutako denbora eta errealitatean sartutako denbora alderatuz.

Azkenik, proiektuan zehar ager daitezkeen arriskuen zerrenda agertuko da, bertan agertzen diren arriskuak bat helden bada, soluzioa erraz aurkitzeko.

## 2.2 Proiektuaren helburuak

---

Proiektuaren helburu nagusia segurtasun kopiak burutzen dituen azpiegitura baten martxan jartzea da. Hori burutzeko, 2.1 irudian agertzen den bezala, zenbait azpi helburu definitu dira.



2.1. irudia. Helburuen laburpena.

1. Aztertu, diseinatu, inplementatu, probatu, balioztatu eta produkzioan jarri *Arcserve UDP* softwarean oinarritutako *Disk to Disk* (D2D) motako segurtasun kopiak burutzen dituen soluzio bat, LYO egoitzan, aurrerago beste egoitzetan aplikatzeko aukera izanik. Gaur egun, *Arcserve Backup* erabiltzen da, honi esker informazioa zintan gordetzen da.

2. *Arcserve UDP* softwarea konfiguratu eta ondorengo zerrendan agertzen diren zereginen *scrip*-tak garatu:
  - a. *Reporting* zereginak automatizatuko dira. Segurtasun kopien egoera eta informazioa gehigarria eskuratuz.
  - b. Segurtasun kopien kontrol automatikoa programatuko da.
3. Segurtasun kopiak burutzen dituen bi programen arteko konparaketa: *Arcserve UDP* eta *Veeam*. Gaur egun enpresan bi soluzioak erabiltzen dira. *Veeam* programaren kasuan, 150 zerbitzariz osatutako *VMWare* multzo batentzat erabiltzen da eta helburua ez da programa hau ordezkatzea, baizik eta *Arcserve*-n onurei dagokionez, noiz dagoen haren beharra bilatzea.
4. Eboluzioak eta uneko azpiegituraren hobekuntzak proposatzea, honi esker efizientzia handiago bat lortuz.

## 2.3 Lan Metodologia

---

Proiektua gauzatzeko jarraian azaltzen den metodologia erabiliko da. Metodologia hau, fase desberdinez osatuta dago.

Hasieran, ezer garatu aurretik, plangintza orokor bat prestatu da, proiektua egiten hasteko plangintza, hain zuzen ere. Plangintza horrek bi helburu nagusi ditu, batetik lana egiten hasteko oinarri bat izatea, eta bestetik, proiektua antolatzeke lehenengo pausuak izatea.

Ondoren informazioa bilduko da iturri desberdinetatik. Bildutako informazioa alderatu eta aintzakotzat hartu diren iturri fidagarriekin egiaztatuko da, ondoren jaso den informazioaren aukeraketak eta bazterketak egiteko.

Analisia eginda dagoela, produktua garatzera pasako da. Produktua garatzerakoan, produktuaren garapenean lagunduko duen informazio berria eskuratzea espero da. Arazorik balego produktuaren garapenean eta konponbidea emateko aukerarik aurkitzen ez bada, hau dokumentatu egingo da, esanez zein izan den edukitako arazoa eta emandako konponbideak. Konponbide horiek lortzeko hurrengo 2.8. atalean agertzen diren gidalerroak erabiliko dira.

Jarraian produktu zein memoriaren jarraipen eta kontrol fasea etorriko da. Produktua garatzen den bitartean, honen kontrolaren dokumentazio bat egitea ezinbestekoa baita. Honen ondorioz, aurredefinitutako helburutik gertu izan naizen ala ez jakin izango dut uneoro. Proiektuan zehar sartutako orduen kontrola izateko taula eguneratzen joan da, desbiderapen konkretuak izateko.

Hori dena garatzeko 3 ingurune ezberdin bereiztu dira:

- *Developement* (DEV): Bertan garapena eta aldaketak egiten dira, kritikoa den zerbitzari batean aldaketa bat egiten baduzu, enpresan ez duela eraginik bermatzeko.

- *Quality Assurance (QA)*: DEV ingurunean burutu diren probak edo inplementazioak probatzeko tokia da.
- *Production (PROD)*: Funtzionamendu egokia egiaztatu denean, ekoizpenean edo beste modu batera esanda, martxan jarriko da garatutako zerbitzu edo aplikazioa.

Aipatzekoa da ere proiektuaren segurtasun kopiak egingo direla, batetik, lainoan eginiko kopiak *Google Drive* plataforman gordeko dira, eta bestetik, kopia lokalak disko gogor batean. Segurtasun kopia hauek astero egitea espero da, baina garrantzizkoa den atal bat garatu bada, segurtasun kopia, atal hori garatutako egunean egingo da.

Garapena burutzen den bitartean, paraleloki memoria idazteari ekingo zaio. Memoria idatzita dagoelarik, hobekuntzak egiteko denbora baldin badago, 300 ordu horiek asebetetzeko, hobekuntzak egiten saiatuko dira. Garapenean arazorik balego eta memoria idazteko denbora justu dagoela estimatzen bada, garapena bertan behera uztearen zergatia eta ematen saiatu diren konponbideak azalduko dira.

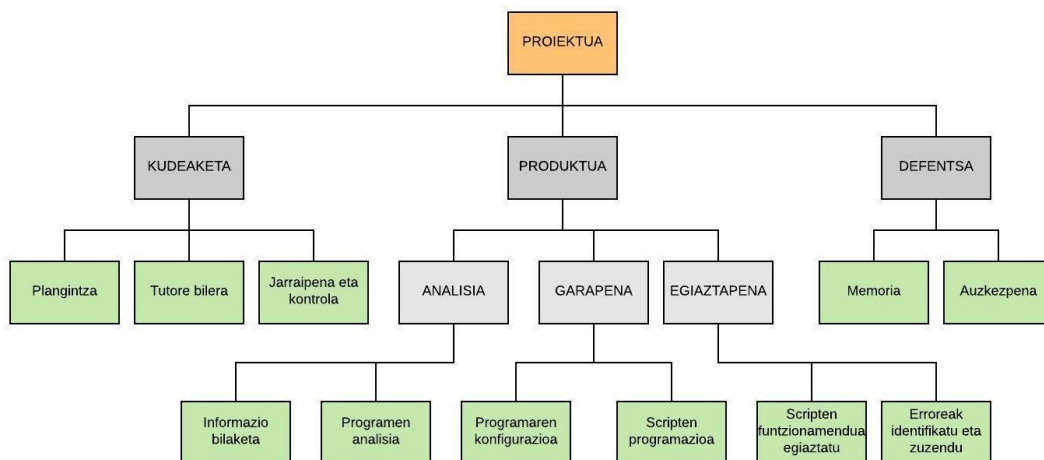
Bukatzeko, memoriaren erreposoa egin da, proiektuaren defentsako atal bezala, eta honen inguruko aurkezpen eta poster bat prestatu da.

## 2.4 Plangintza

Atal honetan proiektua aurrera eramateko gutxienez esleitutako orduak zein atazetan eta noiz inbertituko diren azalduko da. Bestetik, atazak identifikatzeko LDE (*Lanaren Deskonposaketa Egitura*) diagrama bat irudikatuko da hauek denbora erreal batetan noiz garatuko diren azalduko duen *Gantt* diagramarekin batera.

### 2.4.1 Atazen deskonposaketa

Proiektua, 2.2. irudian ikusten den bezala, lan pakete desberdinetan deskonposatuko da.



2.2. irudia. LDE diagrama.

Hauek dira *LDE*-tik abiatuz proiektua arrakastaz burutzeko garatu beharreko atazen zerrenda:

#### A1. Kudeaketa

A1.1. Plangintza : Proiektua aurrera eramateko ezarri diren fase eta oinarri puntuak.

A1.2. Tutore bilerak : Unibertsitateko eta enpresako zuzendariarekin, helburuak, proiektuaren egoera eta bete beharrak eztabaidatzeko bilerak.

A1.3. Jarraipena eta kontrola : Proiektuaren nondik norakoaren berri jakiteko, planifikazioarekin egondako desbiderapenak ikusteko eta proiektuaren eguneroko kontrola izateko ataza.

#### A2. Produktua

A2.1. Analisia : Produktua aurrera eramateko kontzeptu eta aplikazio desberdinen azterketa eta ikasketa.

A2.1.1. Informazio bilaketa : Segurtasun kopiei dagozkien kontzeptuen informazio bilaketarentzako ataza. Bertan, segurtasun kopien abantailak, desabantailak, administrazioa, motak etab. aztertuko dira.

A2.1.2. Programen analisia : Segurtasun kopiak burutzeko behar diren bi programen (*Veeam* eta *Arcserve UDP*) azterketa eta ikaskuntza, bien arteko konparaketa bat eginez.

A2.2. Garapena: Proiektuaren garapena burutzeko jarraitu behar diren faseak.

A2.2.1. Programaren konfigurazioa : *Arcserve UDP* programa konfiguratzeko ataza.

A2.2.2. *Script*-en programazioa : Hainbat segurtasun kopiak burutzen dituzten *script* programatzeko ataza eta beste automatizazio batzuk garatzeko ataza.

A2.3. Egiaztapena : Proiektuaren erreposoa burutzeko ataza.

A2.3.1. *Script*-en funtzionamendua egiaztatu : Programatutako *script*-en funtzionamendu egokia egiaztatu. Behar den momentuan exekututzen direla eta baita ere, behar diren datuak gordetzen direla.

A2.3.2. Erroreak identifikatu eta zuzendu : Azken erreposoa burutzeko ataza.

#### A3. Defentsa

A3.1. Memoria : Proiektuan garatuko den produktuaren dokumentazioa.

A3.2. Aurkezpena : Proiektuan garatuko denaren laburpenaren azalpena.

## 2.4.2 Orduen estimazioa eta egutegia

Proiektuaren LDE-an 2.4.1 Atazen deskonposaketa atalean aurkeztutako atazak burutzeko denboraren estimazioa azaltzen da 2.1. taulan.

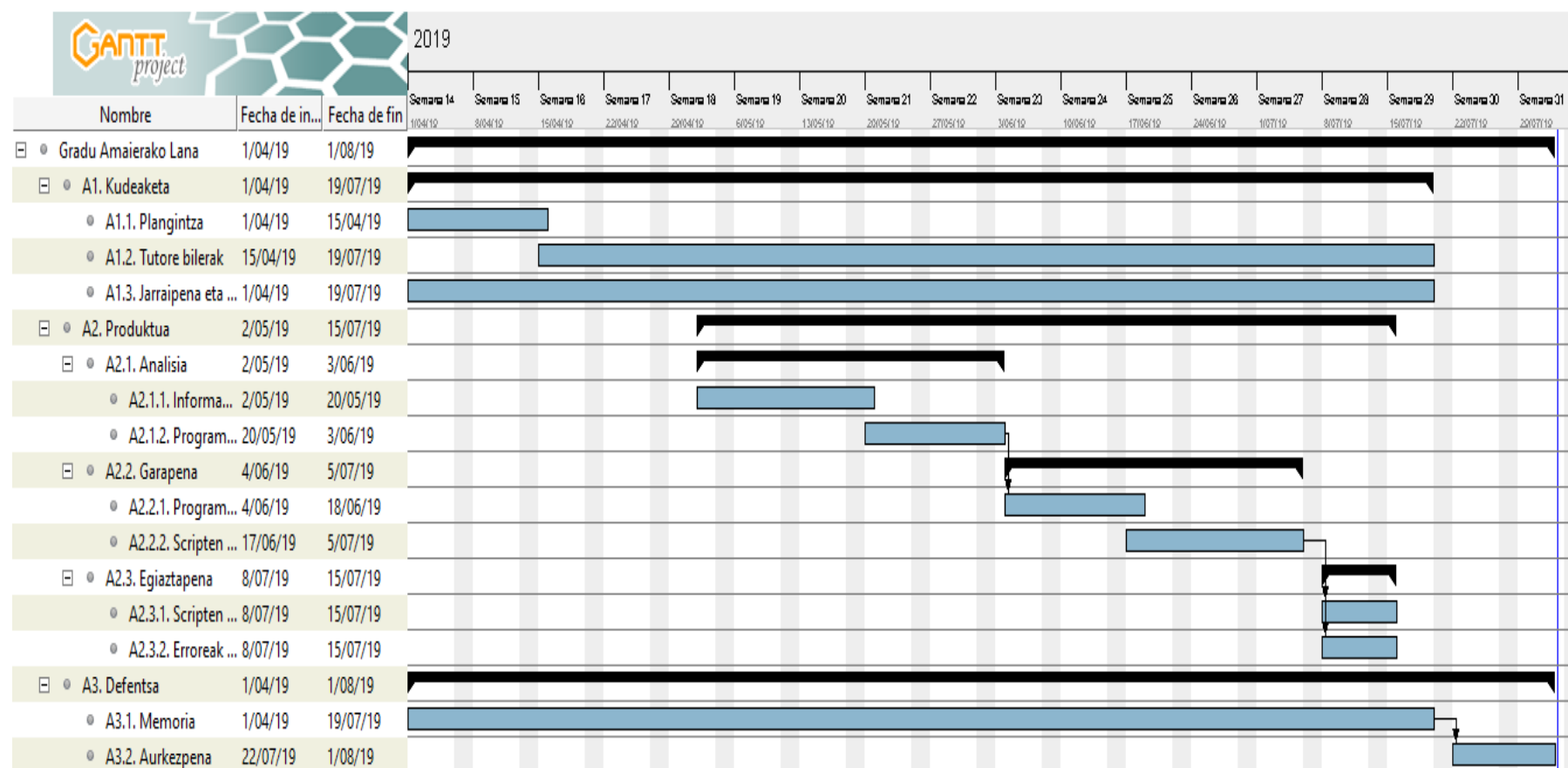
Lan-Paketea	Dedikazioaren estimazioa (ordutan)	Data
<b>A1. Kudeaketa</b>	30	01/04/19 - 19/07/19
A1.1. Plangintza	10	01/04/19 - 15/04/19
A1.2. Tutore bilerak	10	15/04/19 - 19/07/19
A1.3. Jarraipena eta kontrola	10	01/04/19 - 19/07/19
<b>A2. Produktua</b>	175	02/05/19 - 10/07/19
A2.1. Analisia	80	02/05/19 - 03/06/19
A2.1.1. Informazio bilaketa	40	02/05/19 - 20/05/19
A2.1.2. Programen analisia	40	20/05/19 - 03/06/19
A2.2. Garapena	80	04/06/19 - 05/07/19
A2.2.1. Programaren konfigurazioa	40	04/06/19 - 18/06/19
A2.2.2. <i>Script</i> -en programazioa	40	17/06/19 - 05/07/19
A2.3. Egiaztapena	15	08/07/19 - 15/07/19
A2.3.1. <i>Script</i> -en funtzionamendua egiaztatu	10	08/07/19 - 15/07/19
A2.3.2. Erroreak identifikatu eta zuzendu	5	08/07/19 - 15/07/19
<b>A3. Defentsa</b>	100	01/04/19 - 01/08/19
A3.1. Memoria	90	01/04/19 - 19/07/19



A3.2. Aurkezpena	10	22/07/19 - 01/08/19
GUZTIRA	305	01/04/19 - 01/08/19

2.1. taula. Atazen estimazio denborak.

## 2.4.3 Gantt diagrama



2.3. irudia. Gantt diagrama.

## 2.4.4 Arrisku plana

Jarraian proiektuaren garapenean zehar gerta litezkeen arazoak aurreikusi eta hauek nola konpondu planifikatu da. Esan beharra dago arrisku guztiek ez dutela eragin berdina izango proiektuan. Arazoak larritasun mailaren arabera ordenatuta daude, lehena eragina handiena duena izanik.

### A1 - Lanaren atzerapena.

Deskribapena: Lana arrazoi desberdinen ondorioz, finkatu den epea baina beranduago bukatzea.

Larritasun-maila: Altua.

Eragina: Finkatu diren epeak ez errespetatzea.

Konponbidea: Disziplinatua izatea eta benetako epea baino lehen bukatuta izatea, horretarako 2.4.3. atalean benetako epea baino lehen bukatzea finkatu da.

### A2 - Ezagutza falta.

Deskribapena: Proiektuan erabiltzen diren programak edo teknologia erabiltzeko arazoak.

Larritasun-maila: Ertaina.

Eragina: Lana moteltzen da.

Konponbidea: Hainbat egun planifikatu teknologia eta programa berrien ikaskuntzarako.

### A3 - Datuen galera

Deskribapena: Emangarri zehatz baten, batzuen edota dokumentu osoa desagertzea.

Larritasun-maila: Aldakorra, galdurako edukiaren arabera.

Eragina: Lana errepikatu behar izatea.

Konponbidea: Proiektuaren artxibo eta dokumentu guztiak lainoan (*Google Drive*) izateaz gain eta disko gogor batean gordetzeaz gain, segurtasun kopiak burutzea.

### A4 – Hardware matxura

Deskribapena: Zerbitzari baten matxura izatea.

Larritasun-maila: Baxua.

Eragina: Lanaren atzerapena.

Konponbidea: Konpontzen den bitartean, beste atal bat lantzen hastea eta hori burutzea. Hori dela eta, lana paraleloan burutuko da, lana aurreratuz.

## 2.5 Jarraipena eta kontrola

Atal honetan planifikatutakoa dedikatutako denborarekin alderatuko da, izandako desbiderapen nagusiak aipatuz eta hauen zergatiak azalduz.

### 2.5.1 Desbiderapenen taula eta azterketa

Proiektuan aurreikusitako eta benetan dedikatutako orduen arteko konparaketa jasotzen da 2.2. taulan.

Lan-Paketea	Dedikazioaren estimazioa (ordutan)	Dedikatutakoa (ordutan)
<b>A1. Kudeaketa</b>	<b>30</b>	<b>34 (+4)</b>
A1.1. Plangintza	10	15 (+5)
A1.2. Tutore bilerak	10	9 (-1)
A1.3. Jarraipena eta kontrola	10	10
<b>A2. Produktua</b>	<b>175</b>	<b>178 (+3)</b>
A2.1. Analisia	80	80
A2.1.1. Informazio bilaketa	40	40
A2.1.2. Programen analisia	40	40
A2.2. Garapena	80	92 (+12)
A2.2.1. Programaren konfigurazioa	40	45 (+5)
A2.2.2. <i>Script</i> -en programazioa	40	47 (+7)
A2.3. Egiaztapena	15	6 (-9)

A2.3.1. <i>Script</i> -en funtzionamendua egiaztatu	10	2 (-8)
A2.3.2. Erroreak identifikatu eta zuzendu	5	4 (-1)
<b>A3. Defentsa</b>	<b>100</b>	<b>100</b>
A3.1. Memoria	90	90
A3.2. Aurkezpena	10	10
<b>GUZTIRA</b>	<b>305</b>	<b>312 (+7)</b>

2.2. taula. Estimaturako eta dedikaturako denboraren arteko konparaketa.

Atal honetan desbiderapenen azterketa egingo da, gertatu diren desbiderapenen zergatiak azalduz eta aurreikusitako denbora eta benetako denbora alderatuz.

- **Plangintza:** Ataza honetan (+5 orduko) desbideratzea egon da. Arrazoi nagusia, pentsaturik zegoena baino gauza gehiago burutzea izan da, hori dela eta, atal honetan luzatu egin naiz. Gainera, plangintza on bat edukitzea ezinbestekoa iruditzen zait proiektua zuzen eta egoki burutzeko. Bertan igaro dudana denbora, luzaroan eskertu dut.
- **Programaren konfigurazioa:** Ataza honetan desbideratze nabaria egon da. Izan ere, ez da soilik programaren konfigurazioa landu behar izan, azpiegituraren egitura nola izan behar den ere planifikatu behar izan da. Gainera, behin pentsaturako konfigurazian, probatu egin da, funtzionamendu egokia bermatuz. Horretaz aparte, programa konfiguratzeko orduan arazoak egon dira. Horietako zenbait arazo konpontzeko teknikoekin harremanetan jarri behar izan da eta prozesu hori motela izan da, ondorioz atazaren estimazioa luzatuz.
- ***Script*-en programazioa:** Ataza honetan estimaturako denbora baino gehiago behar izan da. Izan ere, sortuta dagoen datu base batean informazioa bilatzea eta aukeratzea zaila izan da. Gainera, *script*-a garatzeko softwarea eta ingurunea (Windows) berria zenez alde zuzeneko ikaskuntza behar izan da.
- ***Script*-en funtzionamendua egiaztatu:** Kasu honetan estimaturakoa baino gutxiago behar izan da. *Script*-a garatzen zen bitartean probak egiten zirelako, erroreak pixkanaka identifikatzeko eta zuzentzeko. Ondorioz, ataza honen helburua soilik *script*-a txukuntzea eta zenbait funtzioen deskribapena adieraztea izan da.



# 3

---

---

## Erabilitako Teknologia

### 3. Erabilitako Teknologiak

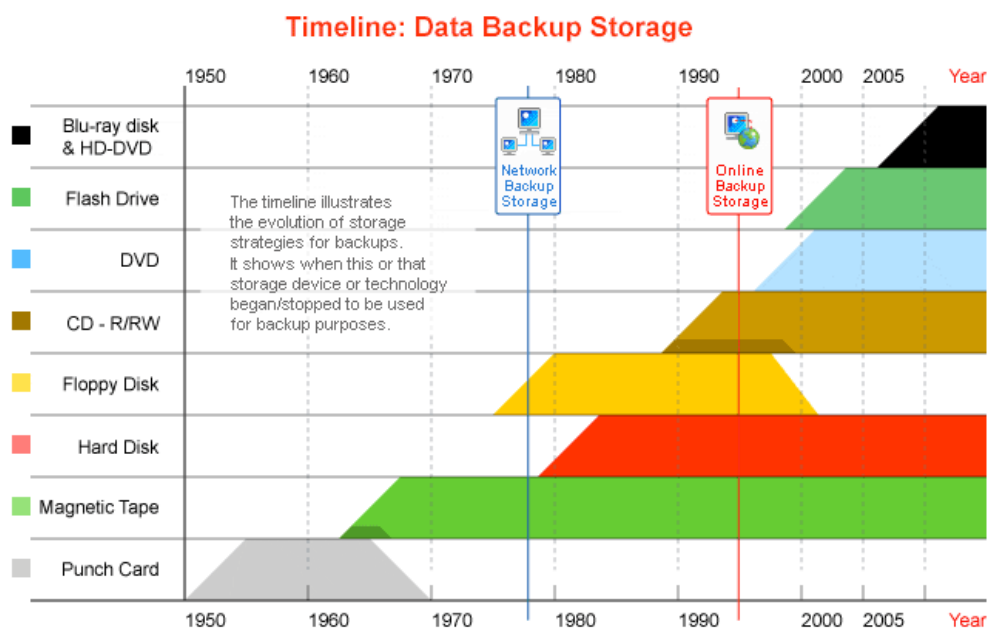
Kapitulu honetan, historian zehar erabili diren biltegitratze gailuen errebasoa egingo da, gaur egun erabiltzen diren gailuetara iritsi arte. Jarraitzeko, *Backup* azpiegitura baten osagaiak zeintzuk diren azalduko dira, baita ere proiektuan erabili den hardwarea eta softwarea zein izan den azalduz. Bukatzeko, garapena burutzerako orduan erabili diren *Backup* mota ezberdinen arteko diferentziak azaldu eta konparatuko dira.

#### 3.1 Aurrekarien analisia

Datu eta informazioaren segurtasun kopiak, gaur egun ere garatzen ari den eremua da. Joera eta irtenbide berriak agertzen dira maiz, segurtasun kopien metodoak eta teknologiak konplexuagoak bihurtuz.

Segurtasun kopien edo datuen segurtasun kopien jatorria zibernetika eta informatikaren sorreratik dator. Orduz geroztik, informazioarekin lan egiten zen bakoitzean, bai ingurune digitalean edo ingurune birtualetan ere, beti segurtasun kopiak egitea beharrezkoa zen, hainbat arrazoiengatik; Batetik, proba batzuk egiteak datu baliotsuen galera ekar zezakeelako. Bestetik, denbora hartako sistemak ez zirelako seguruak ezta eraginkorrak. Gainera, dagoeneko informazio garrantzitsua lapurtzeko mehatxuak existitzen ziren.

Denborarekin, sistema informatikoen bilakaera izan zuten eta etxeetara masiboki heldu ziren. Honek informazio garrantzitsua etxeetan ere edukitzea ekarri zuen eta hori babesteko beharra ere sortu zen. Hori dela eta, biltegitratze euskarri ezberdinak garatzen joan dira informazio fluxua geroz eta handiago zen heinean. 3.1. irudian denboran zehar biltegitratze gailuek izan duten bilakaera historikoa azaltzen da:



3.1. irudia. Teknologien denbora diagrama.

Iturria: <http://www.backuphistory.com/>



**Txartel zulatua**, 1960ko eta 1970eko hamarkadan ordenagailuetan informazioa eta argibideak sartzeko erabilitako lehenengotako teknologia nagusia izan zen. Txartel zulatu bat edo, besterik gabe, txartel bat, kartoizko xafra bat da, kode bitarraren arabera hainbat zuloren bidez informazioa daukana. Esan beharra dago, txartel hauek biltegitzen zuten informazioa minimoa zela, ondorioz, txartel askoren beharra zegoela operazio konplexuetarako.

Ondorioz, akats nagusia une bakoitzean galtzen zen denbora guztia izan zen. Aldi berean, ezin da ahaztu teknologia hau hurrengo urteetan gertatutako garapen guztiaren jaurtiketa izan zela.

Ondoren, **zinta magnetikoak** iritsi ziren. Hauek ezagunak ziren audio eta bideoen grabaketarako, baina ez ziren inoiz erabili informazioa gordetzeko eta ondoren sistemak irakurtzeko. Funtsean, sekuentziak edo pistak kopiatzen ziren plastiko batean material magnetizatuarekin. Zinta magnetikoko bolumen bat 10.000 txartelen datuak gordetzeko gai izan zenez, berehalako arrakasta lortu zuen eta datu informatikoen biltegitik ezagunena bihurtu zen 1980ko hamarkadaren erdialdera arte.

Enpresa handiak eta txikiak segurtasun kopiak zintan sortzen hasi ziren. Zinta magnetikoei esker, segurtasun kopia hedatuagoak sortzea lortu zen, zinta unitateen fidagarritasuna, eskalagarritasuna eta kostu txikia direla eta. Abantaila guzti hauek, gaur egun ere konponbide erakargarria izatea lortzen dute.

Teknologia honen adibiderik ezagunenak, 1960 eta 2000. urteen artean indarrean egon diren **diskete** ospetsuak dira. 1969an lehenengo disketea sortu zen. Diskete honek, soilik 80KBeko tamaina zuen eta gainera, soilik irakurtzeko aukera. Lau urte geroago, 1973an, biltegitatze handiagoa eta idazketa/irakurketa egiteko aukera zuen diskete bat sortu zen. Orduz geroztik, joera bera izan da: diskete txikiagoak eta datu gaitasun handiagoa.

Disketeak euskarri iraultzaile gisa kontsideratu ziren, datuak ordenagailu batetik bestera garraiatzeko. Disketeen segurtasun kopiak ez ziren zintan egiten, baina disko hauek nahiko merkeak eta oso erabilgarriak izan zirenez, azkar bihurtu ziren etxeko erabiltzaile eta enpresa txikien artean segurtasun kopiak burutzeko aukera nagusienetako bat. Gaur egun ez dira erabiltzen artxiboek dituzten tamaina handia dela eta.

1983. urtetik, **disko gogorra** ordenagailu pertsonal gehien osagai bihurtu zen. Beste gertaera garrantzitsua teknologian *Redundant Array of Inexpensive Disks*-en (RAID) sarrera izan zen, 1990. urte hasieran. Datu biltegi horren eskemak, disko gogor ugari erabiltzen ditu datuak haien artean partekatze edo errepikatze. Hobekuntza horri esker, datuak disko gogorretan gordetzea eskuko irtenbide bihurtu da, bai eta oso erakargarria ere.

1960 eta 1970. urteetan, disko gogorrek ez ziren egokiak segurtasun kopiak egiteko, haien prezio altuengatik, tamaina handiagatik eta haien kapazitate txikiarengatik. Bestalde, 1980. urtean disko gogorrek, segurtasun kopiak egiteko baliagarri gisa kontuan hartzen hasi zituzten. 1990. urtearen hasieran, disko gogorrek segurtasun kopiak egiteko alternatiba bihurtu ziren. Gaur egun, zinten eta disko gogorren arteko liskarra mantentzen da.

Hurrengo belaunaldian sortu ziren biltegitratze euskarriek tamaina handiago zuten: CD-Grabagarria (CD-R) eta CD-Idazgarria (CD-RW) unitateak.

1990. urtean CD-Rak ez ziren erabiltzen segurtasun kopiak gordetzeko beraien kostu altua dela eta. Beranduago, CD-ROMak ia ordenagailu guztietarako ohiko gailua bihurtu zenean eta disko trinkoen prezioak nabarmen jaitsi zirenean, segurtasun kopiak gordetzeko erabiltzen hasi ziren.

*Compact disc Read-Only Memory (CD-ROM)* -a, irakurketa mekanismo optikoa jarraitu zuen beste gailu bat izan zen, baina lehenengoa laser bat erabiltzen, datuak biltegitratzeko eta irakurtzeko. Hortaz aparte, materialak askoz ere iraunkorragoak eta gogorragoak ziren. Gainera, biltegitratze tamaina normala handitu zen, disketeen 1,5 MBetik 700 MBera pasatuz.

Denbora igaro ahala, teknologia hau ezaguna bihurtu zen eta azkenengo urteetan zaila da irakurgailu optikorik ez duen ordenagailu bat aurkitzea, software gehienak modu horretan banatu eta instalatzen bait dira. Jakina, aurrerapen teknologikoarekin batera, gaitasunak handitu egin ziren eta beste disko trinko batzuk sortu ziren, hala nola *DVD*ak (4,7 GB) eta egungo *Blue-Ray* (25 GB).

Ondoren *Universal Serial Bus (USB)*-ak iritsi ziren. USB-ak, 1998an asmatu ziren eta informazioa gordetzeko flash memoria bat erabiltzen duten biltegitratze-gailu bat dira. Hasiera batean, hauek sortuak izan zirenean, inork ez zuen ulertzen zertarako balio zuten ezta nola funtzionatzen zuten. Hala eta guztiz ere, denbora pasa ostean ezagunak egiten hasi ziren eta gaur egun oso merke aurki daitezke. Nahiz eta ez ziren asko erabili segurtasun kopiak gordetzeko, oso erabiliak izan ziren datuen biltegitratze pertsonal bezala.

Unitate hauen tamaina, potentzia eta kostu-eraginkortasuna kontuan hartuta, ez da harritzekoa datuen babes merkatuan indar handia izatea. Izan ere, gaur egun 1TBeko tamaina duen USBak aurki daitezke. Hala ere, eramangarritasun izugarriaren ondorioz, oso erraz gal daiteke informazioa askotan erabiltzen denean, bere bidez erabat murriztuz.

Lehenago komentatu den bezala, segurtasun kopien garapena, sareen eta interneteko teknologien garapenarekin lotuta dago. Sare lokalak agertu zirenez, bakoitzaren sistema pertsonaletik urruneko segurtasun kopiak burutzeko aukera sortu zen. Sare lokal eta globalek urruneko sistema baten biltegitratzea gaitzen dute datu kritikoen segurtasun kopiak burutzeko. Hondamendi baten aurrean babesteko, jende askok nahiago du segurtasun kopien fitxategiak urrunera bidaltzea eta gordetzea.

Hona hemen segurtasun kopien asmakizun eta irtenbide garrantzitsuenak:

- ***File Transfer Protocol (FTP)***

Fitxategien Transferentziarako Protokoloa edozein sistema eragileren artean fitxategien elkar-trukatzea ahalbidetzen duen sare protokoloa da. Zehazki, protokolo hau edozein saretan fitxategiak trukatzeko erabilitako protokoloa da. Hori dela eta, ordenagailuen artean datuen kopiak gordetzea errazten du.

- **Network Attached Storage (NAS)**

NAS konputagailu-sare baten bitartez, zerbitzari baten biltegitratze ahalmena, PC-ekin zein beste zerbitzariekin, partekatze teknologia da. Teknologia hau 1980ko hamarkadaren erdialdean agertu zen eta biltegitratze fabrikatzaile handiek beraien produktuetan gehitu zuten, segurtasun kopiak egiteko aukerak barne.

- **Storage Area Network (SAN)**

Biltegitratze eremuko sarea, zerbitzariak, disko multzoak eta babes liburutegiak nagusiki konektatzeko konputagailu sarea da. Abiadura handiko, berehalako eta programagarriak diren segurtasun kopiak eskaintzen ditu enpresa handiei.

- **Lainoa**

Lainoaren kontzeptua Internetekin zuzenean lotuta dago. Laburki esanda, informazioa gordetzeko espazio digital bat da zerbitzari batean. Lainoaren ezaugarriak enpresak jartzen dituen baliabidearen arabera izango da, baina normalean espazio doan bat dago. Bere desabantaila nagusietako bat, Internetera konektatzeko beharra da. Asmakuntza eta garapen guzti hauek datuen segurtasun kopiak egiteko oinarri teknologikoak bihurtu dira.

## **3.2 Backup azpiegitura baten osagaiak**

---

Atal honetan segurtasun kopiak burutzen dituen azpiegitura baten osagaiak azalduko dira.

- Bezeroak: Informazioa edo gorde nahi diren datuak dituzten sistemak.
- *Backup* zerbitzaria(k)
  - Master zerbitzaria: Zerbitzari nagusia da. Bertan datu base bat dago, fitxategien (segurtasun kopien) kontrola eta haien kokalekua daramana.
  - Media zerbitzariak: Zerbitzari osagarriak dira, biltegitratze tamaina handitzeko.
- Biltegitratze gailuak:
  - Lehen mailako biltegitratzea: Bertan ekoizpen-zerbitzarien datuak gordetzen dira. Datu hauek beti *online* egoten dira eta disko gogorretan gordetzen dira.
  - Bigarren mailako biltegitratzea: Bertan segurtasun kopiak gordetzen dira, hau da, *online* dauden datuen errepikapen bat. Mota desberdinetako gailuak erabili daitezke, hala nola, zinta, diskoak, dispositibo optikoak, etab. Bakoitza bere kostu eta errendimendua eskaintzen du.

Proiektuan biltegitratze gailu bezala diskoa eta zinta erabiliko direnez, haien ezaugarri garrantzitsuenak aipatuko dira.

Zintari dagokionez, segurtasun kopiak biltegitzeko gehien erabiltzen den teknologietako bat da, diskoarekin batera. Datuak biltegitzeko ahalmen handia du, energiaren kontsumo baxu batekin. Gailu hauen iraupena ere luzea izaten da, 20 eta 30 urte bitartekoa. Horri esker, segurtasun kopiak kokapen fisiko ezberdin batean gorde daitezke, ekoizpen zerbitzarietatik aldenduta. Idazkera linealeko gailua da, hau da, zinta bi noranzkoetan idazten da. Idazkera mota hau oso egokia da datuzko bloke handiak gordetzeko. LTO (*Linear Tape-Open*), zinta baten adibide bat da. Zinta mota desberdinak daude LTO-1etik hasita LTO-8ra arte. Bakoitza aurrekoarekin konparatuz hobekuntzak eskaintzen ditu, tamaina edo abiadura faktoreetan esaterako. Zinta hauek, zinta unitate batean (zintak irakurtzeko gailua) irakurri behar dira. Gaur egun denak batera aurkitzen dira, *tape library* izeneko leku batean. Liburutegi honetan zintak *slots*-etan gordetzen dira. Zintak tamaina maximora iristen direnean, hauek, *slots*-etatik ateratzen dira zinta hutsak ipiniz. Robot batek zinta bakoitzaren barra-kodea irakurriz, idazten eta irakurtzen du zinta horietan.

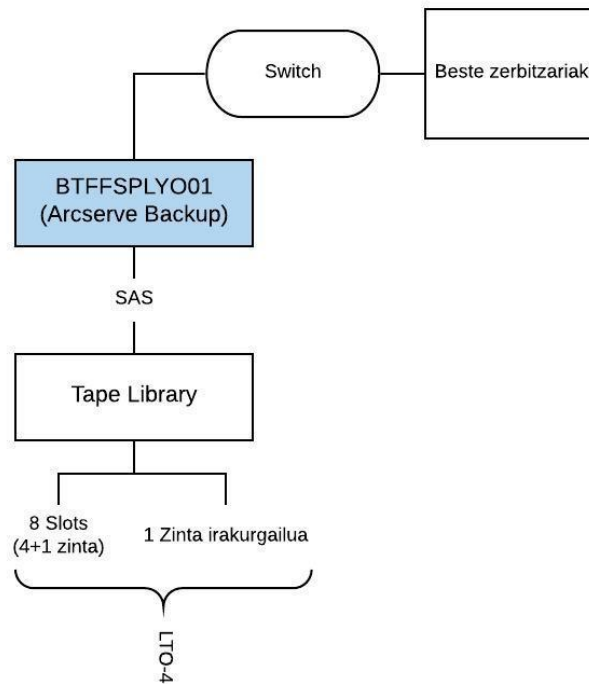
Diskoari dagokionez, bere erabilera asko aldatzen da: unitate sinple bat izan daiteke, bertan informazioa gordetzeko edota deduplikazioa teknika aplikatzeko gailu bat adibidez. Teknika honen bitartez, datu bloke errepikatuak ezabatuko dira, baina soilik aplikatu daitezke errepositorio berdinean dauden kopietarako.

Zintarekin alderatuz, diskoaren kostua nahiko altuagoa da eta energiaren kontsumoa behar dute denbora guztian zehar, hau da, beti funtzionatzen egon behar dute. Diskoa azken finean erabiltzen da, paraleloki karga handiko lanak egin ditzakeelako eta baita ere lehen aipatutako deduplikazio teknika erabili ahal daitekeelako. Hori dela eta, zeregin espezifikotarako erabili ohi da.

Normalean datu asko maneiatzen dituzten enpresetan ez da diskoa soilik erabiltzen biltegitzeko gailu bezala, bere kostu altua dela eta. Ondorioz, nahasketa bat egiten da biak konbinatuz. Diskoan kopiatutako datuak, ondoren zintara pasa ohi dira. Horrela segurtasun kopia egiterakoan, azkarragoa izango da eta ondoren denbora periodo baten ondoren zintara pasako da, diskoaren espazio librea handituz.

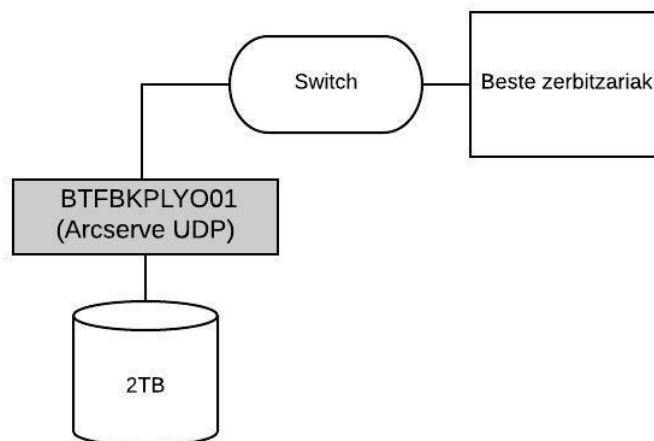
### 3.2.1 Proiektuko azpiegituraren osagaiak

1.2. atalean aipatu den bezala, oraingoz segurtasun kopiak zintan gordetzen dira. 3.2. irudian agertzen den egitura jarraitzen da LYO egoitzan:



3.2. irudia. Zinta azpiegitura.

BTFFSPLYO01 *Backup* zerbitzaria da eta *switch* baten bidez beste zerbitzarietara konektatuta dago. Zerbitzaria eta *tape library Serial Attached SCSI (SAS)* kable baten bidez lotuta dago, honen abiadura teorikoa 6 GB/s-koa izanik, baina hainbat faktoreren ondorioz, gehienez 100 MB/s koa da. Liburutegi hori zinta irakurgailu batekin eta 8 *slot*-ez osatuta dago baina bakarrik 5 *slot* okupatzen dira (4 zinta segurtasun kopiak egiteko eta zinta garbitzaile bat). Erabiltzen diren zintak LTO-4 motakoak dira, bere tamaina 800 GBkoa izanik eta idazteko abiadura 100 MB/s-koa izanik.



3.3. irudia. Disko azpiegitura.

Azpiegitura hau hobetu nahi dugunez, 3.3. irudian agertzen den bezala, oraingoan BTFBKPLYO01 izango da *Backup* zerbitzaria eta bertan *Arcserve UDP* programa instalatuta dago, segurtasun kopiak diskoan burutzeko.

### 3.3 Hardware eta softwarea

---

Proiektuan zehar erabili dudan *Hardwarea* honako hau da:

- Ordenagailu pertsonala :
  - Prozesadorea: Intel Core i5-6200U 2.30GHz
  - Sistema eragilea: Windows 7
  - RAM memoria: 4GB
- LYO egoitzako zerbitzari guztien datuen laburpena 3.1. taulan agertzen dira baina garrantzitsuenak honako hauek dira:
  - **BTFBKPLYO01:** Segurtasun kopiak diskoan burutzeko zerbitzaria (HP ProLiant 360 GEN 8), DEV ingurunean. Honek 2TBko tamaina duen diskoa du. Tamaina hori nahi dudan bezala antolatuko dut eta sistema berrezartzeko baimena izango dut. Zerbitzari honetan *Arcserve UDP* programa instalatuta dago.
  - **BTFBSPLYO01:** Fitxategi zerbitzaria, PROD ingurunean kokatua. Bertan segurtasun kopiak zintan idazten dira eta *tape library* batera konektatuta dago. Zerbitzari honetan ezingo dira aldaketak egin.
  - Egoitzan geratzen diren zerbitzarietan *Arcserve UDP*ren agenteak instalatuko dira BTFBKPLYO01 tik.

LYO egoitzako zerbitzari guztien datuen laburpena:

Zerbitzaria	Ingurunea	C:\	D:\	E:\	APP	OS	Backup Arcserve Backup-ekin?	Backup Arcserve UDP-rekin?
<b>BTFASPLYOAST01</b>	DEV	20 GB	N/A	N/A	Asterisk (VoIP)	Linux	Ez	Ez
<b>btfasplyonex1</b>	DEV	20 GB	N/A	N/A	Nexpose	Linux	Ez	Bai, oraingoz segurtasun kopia osoa.
<b>BTFBKPLYO01</b>	DEV	50 GB	25 GB	N/A	Arcserve UDP	Windows 2012	Ez	Ez
<b>BTFDCPLYO01</b>	PROD	19GB	1 GB	N/A	DC	Windows 2012	Bai, osoa	Bai, oraingoz segurtasun kopia osoa nahiz eta, <i>System State</i> eta <i>DCren</i> artxiboak soilik behar.
<b>BTFFSPLYO01</b>	PROD	30 GB	3 TB	N/A	File Server	Windows 2012	Bai, D:\ Unitatea	Bai, D:\ Unitatea
<b>BTFHSPLYO01</b>	PROD	N/A	N/A	N/A	ESXi Server	VMWare ESXi 6	Ez	Ez
<b>BTFISPLYO01</b>	PROD	16 GB	1.5 GB	N/A	DHCP	Windows 2012	Bai	Bai, oraingoz segurtasun kopia osoa nahiz eta <i>DCHP</i> aren <i>scope</i> -a soilik behar.
<b>BTFISPLYO05</b>	PROD	22 GB	90 GB	N/A	WSUS	Windows 2012	Ez	Bai, oraingoz segurtasun kopia osoa.
<b>BTFISPLYO11</b>	PROD	13 GB	3.5 GB	N/A	Kaspersky	Windows 2016	Ez	Bai, oraingoz segurtasun kopia osoa.
<b>BTFPSPLYO0001</b>	PROD	17 GB	1 GB	N/A	Printer	Windows 2012	Bai	Ez, inprimatzailearen konfigurazioen segurtasun kopiak <i>DTC</i> an burutzen dira.
<b>SASLYO0010</b>	PROD	12 GB	345 GB	10 GB	PLM Teamcenter	Windows 2003	Bai	Ez, laster <i>DTC</i> ra mugituko da.

3.1. taula. LYO egoitzako zerbitzarien datuak.

Proiektuan zehar erabilitako *Softwarea* honako hau da :

- Arcserve UDP (6.5.4175 bertsioa): Segurtasun kopiak sortzeko erabili den programa. Premium lizentzia instalatuta.
- PMP (*Password Manager Pro*): Aipatutako zerbitzarietan urruneko konexioak egiteko aukera ematen duen programa.
- GLPI: Sistemaren informazioa kudeatzeko erabiliko den web aplikazioa da. Programa honen bitartez, zerbitzariak instalatuta dituzten programak eta ezaugarriak ikusi daitezke. Laburbilduz, sistemaren inbentarioa da.
- Trello: Web interfazea duen proiektuen kudeaketarako softwarea da. *Kanban* metodoa erabiltzen du, metodologia azkarra eta eraginkorra bultzatuz.
- Lucidchart: Grafikoak sortzeko programa.
- Power BI : Datu base batetik lortutako datuak era automatiko erraz eta bisual batean ikusteko aukera ematen duen programa.
- Microsoft SQL Server Management Studio: Datu basea kontsultatzeko programa.
- Powershell ISE: *Script*-ak programatzeko erabili den baliabidea.
- Ntop: Sare baten trafikoa monitorizatzeko eta kontrolatzeko erabilitako erreminta.



## 3.4 Motak

Gaur egun, segurtasun kopiak burutzen dituzten programek mota ezberdinetako *Backup*-ak sortzeko aukera dute. Teknika horiei esker datu blokeen tamaina, kopia egiteko denbora eta berreskuratzeko denbora faktoreak aldaera desberdinak dituzte momentuan komeni den teknika erabili ahal izateko. 3.2. taulan azaltzen dira zeintzuk diren mota ezagunenak eta haien abantailak eta desabantailak.

Mota	Datuak	Kopia egiteko denbora	Berreskuratzeko denbora	Biltegiratze tamaina
Osoa	Datu guztiak	Oso motela	Azkarra	Handia
Inkrementala	Aldatutako datuak	Azkarra	Ertaina	Txikia
Diferentziala	Osoatik aldatutako datuak	Ertaina	Azkarra	Ertaina
Ispilua	Aldatutako datuak	Oso azkarra	Oso azkarra	Oso handia

3.2. taula. Segurtasun kopien moten laburpena.

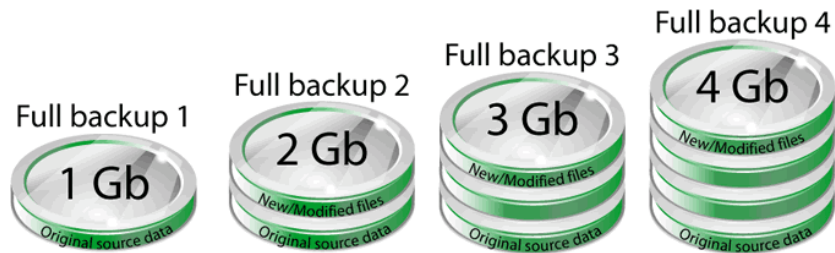
### 3.4.1 Segurtasun kopia osoa

Funtsezko datuen kopia osoa egitean datza. Mota honen erabileraren abantaila nagusia, babeskopia-unitate batean fitxategi eta karpeta guztien segurtasun kopia dagoela da. Ondorioz, azkar eta erraz berreskuratuko da datu guztien segurtasun kopia. Denbora hau, *Recovery Time Objective* (RTO) parametroak neurtuko du.

Hala eta guztiz ere, segurtasun kopia osoa egiteko denbora gehiago behar du beste mota batzuekin alderatuz eta gainera, kopiak tamaina handia izango du.

Hori dela eta, segurtasun kopia osoa, normalean, periodikoki programatzen da, igandero adibidez. Datuen (edo aplikazio kritikoen) bolumen txiki bat kudeatzen duten datu-zentroek, egunero edo maizago burutu dezakete kopia osoa. Ohikoena kasu hauetan, segurtasun kopia inkrementala edo diferentzialarekin konbinatzea da.

3.4. irudiak lau iterazio, hau da, lau segurtasun kopia burutu ondoren, funtzionamendua nola izango den erakusten du.



3.4. irudia. Segurtasun kopia osoaren funtzionamendua.  
Iturria: <https://www.backup4all.com/backup-types-kb.html>

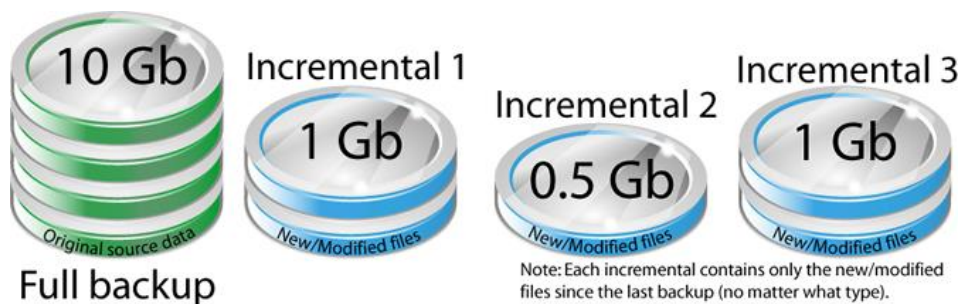
### 3.4.2 Segurtasun kopia inkrementala

Aurreko kopia kontsideratuz (segurtasun kopia inkrementala edo osoa) aldatu diren datuen kopia egiten du.

Adibidez, segurtasun kopia osoa astelehen gauean egiten bada eta astearte gauen inkrementala aldiz, astelehen gauetik aldatu diren fitxategiak soilik kopiatuko dira. Asteazkenean, beste kopia inkremental bat egiten bada, soilik, astearte gauean aldatu diren datuak gordeko dira. Horrela, zure datuen kopiak sarriago egin ditzakezu espazio gehiegi gabe eta exekutatzeko denbora motza izanik.

Datuak berreskuratzeko prozesua aldiz, motelagoa da. Egun jakin baten kopia berrezartzeko, azken kopia osoa eta ondorengo kopia inkremental guztiak berreskuratu behar dira nahi den egunaren kopiaraino iritsi arte. Gainera, horietako kopia inkremental bakar batek arazoren bat badu, ezingo da berreskuratu informazio guztia eta zenbait kasutan bat ere ez.

3.5. irudiak lau iterazio, hau da, lau segurtasun kopia burutu ondoren, funtzionamendua nola izango den erakusten du.



3.5. irudia. Segurtasun kopia inkrementalaren funtzionamendua.  
Iturria: <https://www.backup4all.com/backup-types-kb.html>

### 3.4.3 Segurtasun kopia diferentziala

Segurtasun kopia mota honetan, inkrementalarekin alderatuz, azken kopia osoan aldatu diren datu guztien kopia egiten da. Adibidez, kopia osoa astelehenean egiten bada eta asteartean kopia diferentziala programatzen bada, denbora tarte horretan aldatu diren datuen kopia egingo da. Asteazkenean beste bat programatzen bada, kopia osoarekin alderatuz, aldatu diren datu guztien kopia egingo da, hau da, berriro ere astearteko datuen kopia egingo da. Ondorioz, kopia hauek tamaina handitzen joango dira. Datu gehiago kopiatu behar direnez denbora ere luzeagoa da.

Berreskurapen prozesua aldiz errazagoa da, soilik azken kopia osoa eta azken kopia diferentziala berreskuratu behar bait dira. 3.6. irudiak lau iterazio, hau da, lau segurtasun kopia burutu ondoren, funtzionamendua nola izango den erakusten du.

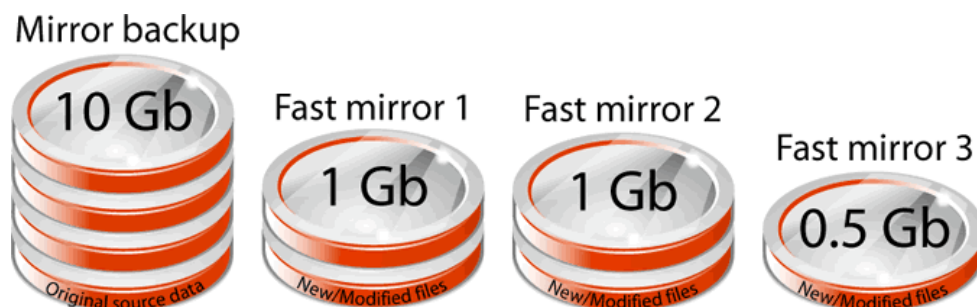


3.6. irudia. Segurtasun kopia diferentzialaren funtzionamendua.

Iturria: <https://www.backup4all.com/backup-types-kb.html>

### 3.4.4 Ispiluaren segurtasun kopia

Segurtasun kopia osoaren antzekoa da. Tamaina handia dute eta gainera ez dira hain seguruak. Normalean, iturburuko datuen kopia zehatza sortzeko erabiltzen da. Kopia mota honek ere soilik aldatu diren datuen kopia gordeko du lehengo kopia oso baten ondoren. 3.7. irudiak lau iterazio, hau da, lau segurtasun kopia burutu ondoren, funtzionamendua nola izango den erakusten du.



3.7. irudia. Ispilu segurtasun kopiaren funtzionamendua.

Iturria: <https://www.backup4all.com/backup-types-kb.html>

Laburbilduz, segurtasun kopia mota bakoitzak modu desberdinean funtzionatzen du. Argi dago beti kopia oso bat burutu behar dela eta ondoren konbinatu, bakoitzak nahi duen periodoarekin, kopia inkrementalarekin edo diferentzialarekin. Enpresa, pertsona edo erakunde bakoitzak bere estrategia jarraituko du. Estrategia tipikoak honako hauek izaten dira:

- Kopia osoa + Inkrementala (egunero)
- Kopia osoa + Diferentziala (egunero)

# 4



## Analisa

## 4.1 Segurtasun kopiak burutzeko programen ezaugarriak

---

Segurtasun kopiak burutzen dituzten programa guztien artean, oinarrizko ezaugarriak eta ezaugarri komunak aztertu behar dira. Ezaugarri hauek izango dira konparatuko direnak eta segurtasun kopiak burutzen dituzten programa desberdinek bermatu beharko dituztenak. Ezaugarri horiek ondorengoak dira:

- Segurtasun kopia eta berreskuratze-koherentzia ziurtatzea.

*Backup* programa guztiek, datu kritiko guztiak gorde daitezkeela eta errekueratu daitezkeela ziurtatu behar dute.

- Zerbitzuaren eta negozioaren jarraipena bermatzea.

*Backup* programa guztiek, nahiz eta datu katalogoarekin edota programa berarekin arazo bat eduki, segurtasun kopiak berreskuratze eta berreraikitze gai direla ziurtatu behar dute.

- Informazioaren segurtasuna bermatzea.

*Backup* programa guztiek, segurtasun kopietan biltzen diren datuen konfidentziasuna, integritatea eta autentikazioa bermatu beharko dute.

- Negozioaren beste aplikazioarekin bateragarritasuna ziurtatzea.

*Backup* programa guztiek, aplikazio kritikoaren bateragarritasuna bermatu behar dute, negozioak jarraitasuna edukitzeko. Adibidez, enpresa batek datu base bezala *Oracle* erabiltzen baldin badu, *Backup* programa hori bateragarria izan behar da *Oracle*-rekin segurtasun kopia egiteko.

- Memoria ziurtatzea.

*Backup* programa guztiek, datuak mota bateko gailu batean (zinta, diskoa edota lainoa) gutxienez gordetzeko aukera izan behar dute.

- Automatizazioaren eta informazioaren atxikipena ziurtatzea.

*Backup* programa guztiek, segurtasun kopien eta errekuerazioaren programazio automatikoa eta babestutako datuak ez direla ezabatuko bermatu behar dute.

- Txostenak sortzeko aukera eta erabilera egokia ziurtatzea.

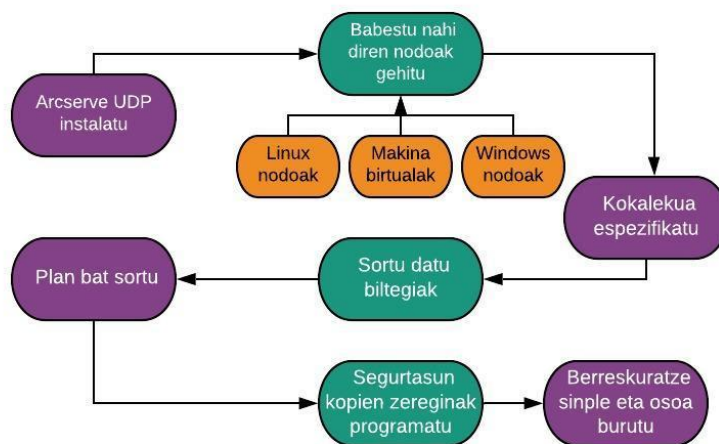
*Backup* programa guztiek, erabilera intuitiboa eta bizia izatea bermatu behar dute. Gainera, txostenak sortzeko eta estatistikak erakusteko gai izan behar dira.

## 4.2 Software aukeraketa

*Backup* azpiegitura bat osatzeko segurtasun kopiak burutzen dituen programa bat eduki behar da. Proiektu honetan, **Arcserve UDP** programa erabiliko da, enpresak, honen lizentzia baitauka. Programa hau, oso eraginkorra da *Information technology* (IT) konplexuetako inguruneak babesten. Windows edo Linux sistema eragileetan dauden datuak babestu ditzake, baita makina birtualetan daudenak ere. Jarraian programaren analisi zehatzagoa egingo da.

### 4.2.1 Funtzionamendua

4.1. irudian agertzen diren pausoak jarraitu behar dira, nahi diren sistemak babesteko:



4.1. irudia. Arcserve UDPren funtzionamendua.

1. Arcserve UDP instalatu.
2. Babestu nahi diren nodoak gehitu programara. Makina birtualak eta Windows edo Linux nodoak gehitu daitezke *ESX/Vcenter* y *Hyper-V* zerbitzarietan.
3. Kokalekua espezifikatu. Segurtasun kopiak non gordeko diren espezifikatu. *Recovery Point Server* (RPS) bat izan daiteke, hau da, zerbitzari bat edota karpeta lokal edo partekatua.
4. Datu biltegiak sortu. Datu biltegia disko baten eremu fisikoa da. Datu biltegiaren deduplikazio teknika aplikatu daiteke.
5. Plan bat sortu. Plan bat, segurtasun kopia kudeatzeko, deduplikazioa kudeatzeko, berreskuratze puntuko kopia kudeatzeko etab. zereginen multzoa da.
6. Segurtasun kopien zereginak programatu.
7. Berreskuratze sinple eta osoa burutu.

## 4.3 Deduplikazioa

---

Datuen deduplikazioa, kopia berdinen ezabaketa burutzen duen teknologia da, honi esker, biltegitratze tamaina murriztuz. Oso erabilgarria eta eraginkorra da datu asko dituzten enpresetan, beti ere, beraien arazoa datuak biltegitratzeko tamaina baitda.

Teknika honek errepikatutako datuak ezabatzen ditu eta hauei erreferentzia egiten dien instantzia bat soilik gordetzen du. Adibidez, 100 erabiltzaile desberdinentzako 10MBeko tamaina duen arxibo berdin baten segurtasun kopia egiten badugu, honek 1000MBeko tamaina izango du. Teknika hau aplikatzen badugu, kopiak gutxi gorabehera, 10MBeko tamaina izango du instantzia bakar bat gordeko delako. Beste 99 instantzietan, gordetako instantziari egingo diote erreferentzia.

Teknikaren abantailak asko dira, hauek honakoak dira:

- Segurtasun kopietan datu gehiago gordetzeko aukera.
- Saretik bidaltzen diren datu kopurua murrizten du.
- Sareko banda zabalera murrizten du.
- Segurtasun kopia azkar egiten da, soilik instantzia gordetzen delako.

### 4.3.1 Motak

*Arcserve UDP* programa bi mota hauekin bateragarria da:

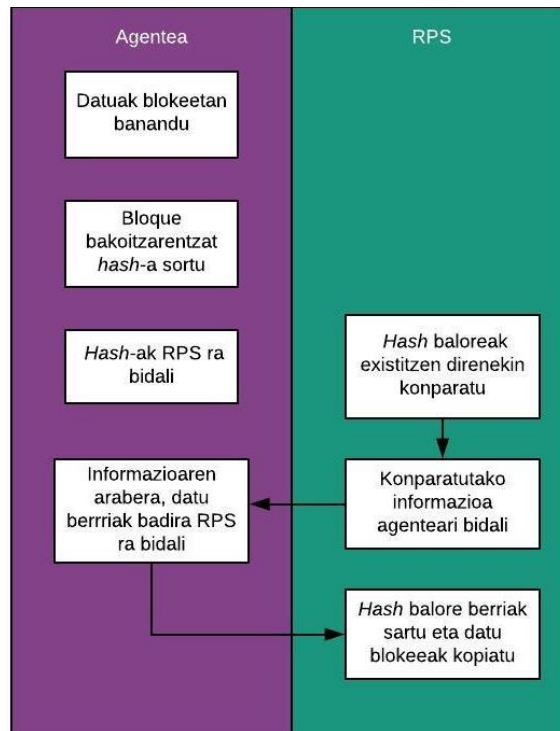
- Deduplikazioa datuen jatorrian: Lehenagotik sortu diren datu blokeen eta sortu nahi diren datu blokeen arteko konparaketa egiten da jatorrian. Hori dela eta, agenteak RPSra bidaltzen dituen datuak, bakarrak eta berriak izango dira. Mota hau oso erabilgarria da bi zerbitzari hauen arteko sare konexioa motela denean. Esan beharra dago, prozesu honek jatorriko sisteman kostu bat duela, izan ere, saturatu daiteke behar dituen baliabideak ez baditu.
- Deduplikazio globala: RPSan dauden datu berrien segurtasun kopia burutzea bermatzen du. Datu bloke berdinak hainbat nodotan badaude soilik segurtasun kopia bat egingo da.

Proiektuan, egoitza bereko nodoen segurtasun kopiak burutzeko deduplikazio globala erabiliko da. Bertan, nodoen arteko sare konexioa LAN bidez denez, konexioa azkarra da. Beste egoitza bateko nodo baten kopia egiteko aldiz, beste mota erabiliko da, sare konexioa (MPLS), motela baitda.



### 4.3.2 Funtzionamendua

Prozesu honek, datuak datu blokeetan banatzen ditu eta bloke bakoitzari identifikadore bat ezartzen zaio. Identifikadore honi *hash* deritzo. Blokeen hasierako tamaina 4KBeko da. *Hash* balore hauek aurretik gordeta dauden beste *hash* baloreekin konparatzen dira era erreferentzi errepikatuak aurkitzen badira, ez dira datu horien segurtasun kopiak burutzen. 4.2. irudian agertzen da deduplikazio prozesuak dituen faseak agente eta RPS artean.



4.2. irudia. Deduplikazioaren funtzionamendua.

Agente gehiago dauden kasuetan, prozesua berdin jarraitzen da, baina agenteen datu errepikatuak filtratzen dira.

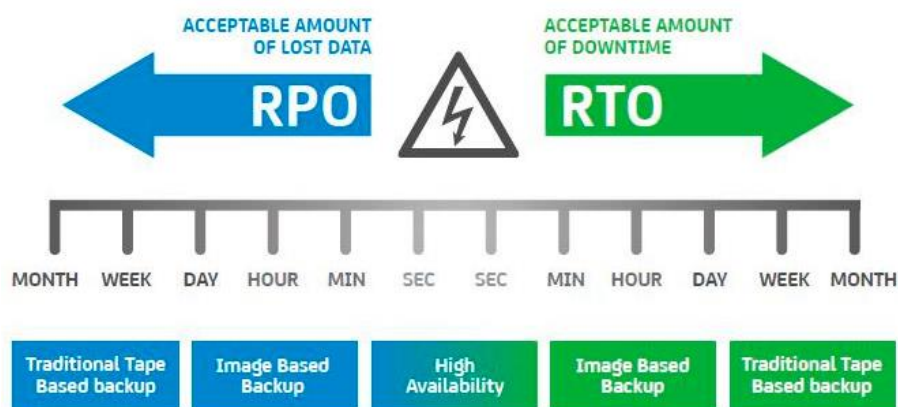
### 4.3.3 Noiz erabili

Hauk izan daitezke teknika honen onuraz baliatzeko zenbait egoera:

- Antzeko datuak dituzten nodoak daudenean.
- Nodo baten segurtasun kopia osoa maiz egin behar denean, kopia egiteko denbora murriztuz.
- Sarearen banda zabalera baliotsua denean, sarean zehar bidaltzen diren datuak murriztuz.
- Datu batzuen segurtasun kopiak nodo batetik bestera maiz aldatzen direnean.

## 4.4 Errekuperazio plana

Hondamendien aurrean errekuperazio plana, sistemak eta aplikazioak %100 funtzionatzea bermatzen duen prozesua da. Plana ondo finkatzea eta ezartzea oso garrantzitsua da, informazioa ez galtzeko edo zerbitzuak geldirik ez egoteko. Edozein motako arazo baten aurrean, prestatuta egon behar da horri aurre egiteko. Prozesu honetan *Recovery Point Objective* (RPO) eta *Recovery Time Objective* (RTO) parametroak aurkitzen dira, 4.3. irudian ikusten den bezala, prozesua planifikatzeko oinarri bezala.



4.3. irudia. RPO eta RTO konparaketa.

Iturria: <https://www.2ksystems.com/blog/14-blog-sistemas-servidores/199-diferencia-entre-rpo-y-rto>

### 4.4.1 RPO

RPO parametroak enpresa batek gal ditzakeen datuak adierazten ditu, hala ere, funtzionamenduan jarraituz. Parametro honek, hondamendi bat gertatzen den momentutik gal daitezkeen datu maximora iritsi baino lehenagoko denbora tartea definitzen du.

Kontzeptua hobeto ulertzeko adibide bat azalduko da. Egunero gaueko 22:00etan segurtasun kopia bat burutzen da. Hurrengo eguneko 11:00etan arazo bat dago datu galera eraginez. Beraz, denbora tarte horretan sortutako datuen galera izango da. Ondorioz, 13 orduko lana galduko da. Kasu honetan, RPO parametroa 24 ordukoa da.

Garrantzitsua da kontuan izatea geroz eta RPO txikiagoa izan, orduan eta maizago egin beharko direla segurtasun kopiak, ondorioz, datuek diskoaren tamaina handiagoa okupatuz.

## 4.4.2 RTO

RTO parametroa hondamendi baten ondoren, sistema batek errekuaratzeko behar duen denbora da, hau da, arazoa gertatzen den momentutik sistema berriro funtzionamenduan hasi bitarteko denbora.

RPO parametroa bezala, honetan ere ahal den denbora baxuena ezartzea komeni da. Horrela, arazo batek sisteman eragin txikia izateko. Denbora murrizteko, faktore askok dute eragina, hala nola, segurtasun kopiaren kokalekua (zinta, diskoa ...).

## 4.4.3 Nola definitu RTO eta RPO parametroak

Plan ezberdinak sortu daitezke parametroak ezartzeko. Planifikazio tipikoena, aplikazio eta zerbitzuen mailaren arabera banatzea da eta parametro hauek ezartzea *Service Level Agreement* (SLA)-aren arabera. SLA, zerbitzua eskaintzen duen ekoizlearen eta bezeroaren arteko kalitatezko zerbitzua bermatzen duen hitzarmena da. Enpresek beti bete beharko duen akordioa da.

Hau ezagutuz hiru maila ezberdinetan banatzen dira aplikazioak:

- 1. maila: Negozioarentzat kritikoak diren aplikazioak. 15 minutu edo gutxiagoko RTO eta RPO-ak ezartzen dira.
- 2. maila: Oinarrizko aplikazioak. 2 orduko RTO-a eta 4 orduko RPO-a ezartzen da.
- 3. maila: Oinarrizkoak ez diren aplikazioak. 4 orduko RTO-a eta 24 orduko RPO-a ezartzen da.



5



Garapena

## 5.1 Proba fasea

---

Lehenengo fase honetan, 4.2.1. atalean zehaztutako pausoak *Arcserve UDP* programan aplikatuko dira. Egoitzaren zerbitzari guztiei aplikatu ordez, lehendabizi soilik **BTFISPLYO05** nodoari aplikatuko zaio konfigurazioa. Zerbitzari hau kritikoa ez denez, segurtasun kopiak edozein momentutan egiteko aukera dago, baita hauek berreskuratzeko aukera ere. Hori dela eta, probak egiteko nodo aproposena da. Ondoren bigarren fasean, zerbitzariaren funtzionamendu egokia bermatu ostean, egoitza guztiari aplikatuko zaio konfigurazioa, beharrezkoak diren plan guztiak sortuz. Konfigurazioa ondorengoa da:

### 1. Nodoak gehitu.

Lehenengo probak egiteko, soilik BTFISPLYO05 nodoa gehituko da kontsolara, programa bera instalatuta duen nodoa ere gehitu beharko da.

Nire kasuan, *Active Directory* bitartez lortu dira egoitzako nodoak. Horren abantaila da egoitza honetan, beste nodoren bat gehituz gero, automatikoki *Arcserve UDP* programaren kontsolan agertuko dela eta beraz, ez dela beharrezkoa era manualean nodoa sartzea.

### 2. Agenteak instalatu nodoetan

Nodo bakoitza agente baten bidez konektatuko da kontsolara, beraz, hauek nodo guztietan instalatuta egotea beharrezkoak dira.

### 3. Kokalekua espezifikatu

Segurtasun kopiak, kontsola instalatuta dagoen zerbitzarian bertan gordeko dira. Zerbitzari hori, hau da, BTFBKPLYO01, RPS bat izango da.

### 4. Datu biltegiak sortu

RPS zerbitzari horretan datu biltegi bat sortu da, zehazki, E:\ unitatea sortu da "Backup" izenarekin, segurtasun kopia guztiak disko partizio berebanean gordetzeko.

Lehenik eta behin, aplikazio baten bidez, datuak biltegiratzeko kokalekuak behar duen tamaina eta *hash*-entzako kokalekuak behar duen tamaina kalkulatu da. Pauso hau oso garrantzitsua da, izan ere, estimatutako memoria ez bada nahikoa, datu berriek ezingo dute *hash* berria sartu datu basean. Hortaz, ezingo dira datu blokeen *hash*-ak konparatu, deduplikazio tasaren jaitsiera bat sortuz.

Babestu diren zerbitzarien tamaina estimatu da. 5.1. irudian ikusten den bezala lehenengo fase honetan datuak ondorengoak dira:

- BTFISPLYO05 → 112GB
- Totala → 3000GB

**Estimate Memory and Storage Requirements**

Enter the estimated values for the amount data to be stored, and the percentage of data that can be deduplicated and compressed. The tool will then estimate the required data destination space, hash destination space, and hash memory space.

[About Deduplication and Compression](#)

Estimated Size of Data to be Stored: 20GB (slider to 100000GB) [300]

Estimated Percentage of Data that can be Deduplicated: 0% (slider to 100%) [20]

Estimated Percentage of Data to be Compressed: 0% (slider to 100%) [30]

Hash destination is on a Solid State Drive(SSD)

Deduplication Block Size: 16KB

Estimated Data Destination Space: 168.0 GB

Estimated Hash Destination Space: 0.6 GB

Estimated Minimum Hash Memory Allocation: 614.4 MB

OK

5.1. irudia. Tamaina estimazioa.

Zerbitzariaren tamaina borobilduz, 120 GBko tamaina du. Kasu txarrenerako, astelehenetik ostiralera, egunero, kopia osoa egiten bada, gehienez 23 egun izango lirateke. Beraz, totalen 2760 GB izango litzateke.

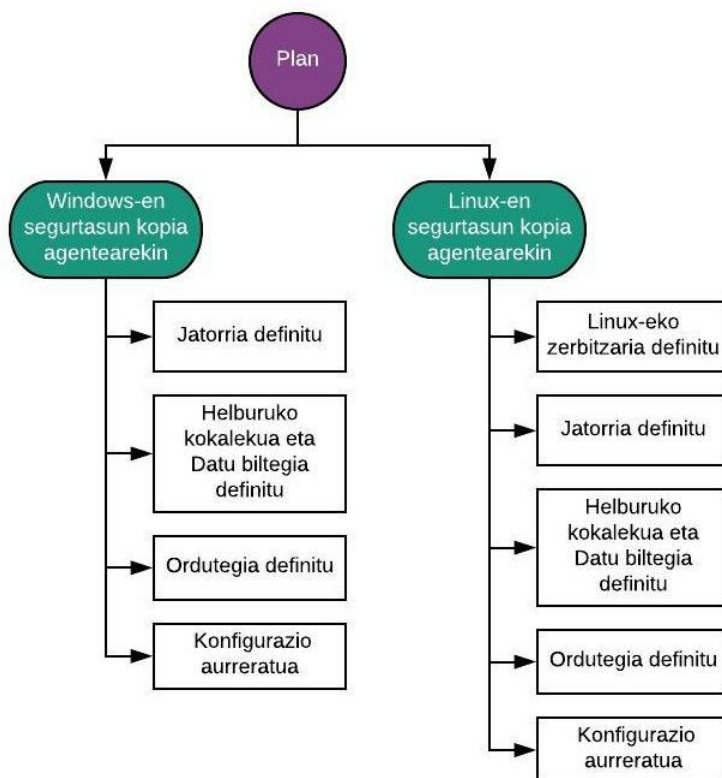
Ondoren, deduplikazioa zenbat daturi aplikatuko zaien estimatu da. Kasu honetan, soilik, zerbitzari bati aplikatuko zaionez deduplikatzen den ehunekoa ezin da oso altua izan, ez daudelako datu asko. Zerbitzari gehiago dauden kasuetan aldiz, deduplikatzen den ehunekoa altuagoa izango da, datu gehiago daudenez datu errepikatu gehiago egongo direlako. Horrekin batera, zenbat datu konprimituko diren eta deduplikazioaren blokeen tamaina (16KB) ezarri da. Konprimaketa teknika ere erabili da diskoaren tamaina murrizteko. Honek kontrako efektu bat ere badu, izan ere, CPU aren erabilera handiagatik, segurtasun kopia burutzeko denbora handiagoa beharko du.

Azkenik, E:/ unitatean 4 karpeta sortu dira:

- Data: Babestutako datuak gordetzeko karpeta. Bertan datu blokeak gordeko dira.
- Index: Indizeak gordetzeko karpeta.
- Hash: *Hash* artxiboak gordetzeko karpeta.
- Data Store: Segurtasun kopiak gordetzeko karpeta.

## 5. Plan bat sortu

Plana sortzerako orduan, sistema eragilearen arabera, konfiguratu beharreko parametroak ezberdinak izango dira. 5.2. irudian azaltzen da plan bat konfiguratzeko prozesua.



5.2. irudia. Plan bat sortzeko prozedura.

BTFISPLYO05 nodoari soilik aplikatu zaio plan hau, lehendabiziko probak burutzeko. 3.1. taula kontsultatuz, oraingoz sistema osoaren segurtasun kopia burutuko da. Segurtasun kopiak, aurreko pausoen sortutako RPS-an, zehazki BTFBKPLYO01 zerbitzarian kokatua, gordetzen dira. Zerbitzari horri, honako plangintza aplikatu zaio:

- Segurtasun kopia inkrementala → Astelehenetik - Ostiralera, 22:00etan.
- Segurtasun kopia osoa → Hilabeteko azken ostiralean, 22:00etan.
- *Verify* segurtasun kopia → Asteartetik- Larunbatera, 1:45etan.

Lan egunak astelehenetik - ostiralera direnez, hauetan kopia inkrementala egiten da, azkarra delako eta tamaina txikiko kopiak sortzen direlako. Gainera, egun batetik bestera egiten diren aldaketak normalean ez dira oso handiak, hori dela eta, ez du merezi egunero kopia oso bat burutzea. Kopia hauek, lan orduetatik kanpo programatu dira, baliabide asko erabiltzen dituztelako. Hala egingo ez bazen, gerta liteke langileen lana oztopatzea eta moteltzea. Kopia hauek 23 egunez gordeko dira, gehienez 23 lan egun izan ditzakelako hilabete batek.



Hilabeteko azken ostiralean, kopia osoa egingo da. Egun horretarako programatu da, prozesuak iraupen luzea duelako, beraz, larunbatean lan egiten ez denez denbora gehiago dago kopia burutzeko. Kopia hau burutu ostean, hilabeteko beste kopia inkrementalak ezabatuko dira, horrela diskoaren espazio librea handituz. Hilero burutzen diren kopia hauek 24 hilabetez, hau da, bi urtez, gordeko dira, bezeroak zehaztutako erretentzio faktorea errespetatuz.

Planteamendu honen arazo nagusia, eguneroko kopia inkremental batean akatsa izatea da. Hori gertatuko balitz, akatsa sortu den egunetik aurrera, ezingo dira beste kopiak erabat berreskuratu eta kasu okerreanean, ezingo da ezer ere ez berreskuratu. Kopia inkremental batean arazoak edukitzeko tasa oso txikia denez, planifikazio honekin jarraitu da. Gainera, arazo hau ekiditeko, egunero, segurtasun inkrementala burutu ostean, *Verify* motako funtzioa exekutatu da. Funtzio honek, azkeneko segurtasun kopia hartuko du oinarri bezala eta azkeneko segurtasun kopiarekin konparatuko du datu bloke bakoitza. Datuak ez badute bat egiten, programak kopia hau aldatuko du bat ez datorren datuak kopiatuz.

Pentsatutako beste planifikazio bat, ostiralero kopia osoa egitea izan litzateke, asteko kopia inkrementalak ezabatuz. Kasu horren arazoa zera da, hurrengo astean langile batek lehengo asteko egun zehatz baten kopia berreskuratzea eskatzen badu, soilik ostiraleko kopia osoa izango duela. Ondorioz, erabilgarritasuna txikia da. Egoera hau aurrekoarekin alderatuz ordea, segurtasun handiagoa du, astero kopia osoa egiten denez, kopia batek akatsa badu, soilik aste bateko datuak gal daitezkeelako.

Prozesua ondo hasteko, lehenengo segurtasun kopia oso bat burutzeko data ezarri behar da abiapuntu bezala. Dena ondo doala egiaztatzeko, segurtasun kopia bukatzean korreora abisu bat bidaltzeko konfiguratu da. Hala eta guztiz ere, kontsolara sartzen den bakoitzean hainbat grafiko azaltzen dira, emaitzen estatistikak adieraziz.

## **6. Segurtasun kopia programatu**

Aurreko atalean programatutako planaren bitartez era automatikoan zehaztutako egun eta orduan burutzen dira segurtasun kopiak.

## **7. Segurtasun kopiaren egoera aztertu**

Lehenengo egunean programatu ziren segurtasun kopiak (segurtasun kopia osoa eta *Verify* funtzioa) ez dira sortu. Errore mezua hurrengoan izan da:

*“License failure”* eta *“Backup job failed”*.

Arazo hau konpondu eta gero, lizentzia berria sartuz, berriro aplikatu zaio plangintza. Kasu honetan, segurtasun kopia burutu da baina *Verify* funtzioa ezin izan da exekutatu programatutako orduan, oraindik kopia burutzen ari baizen. Kopia burutu bezain pronto, hasi da exekutatzen. Hori dela eta, plana aldatu behar izan da, funtzioa beranduago exekutatzuz.

Fase finala planifikatzen hasi baino lehen, proba honen bitartez, *Verify* funtzioa ez egitea erabaki da, asteko segurtasun kopien *log*-ak aztertuz, funtzio hau exekutatu ordeztuz segurtasun kopia

osoa burutzen zela ikusi delako. Izan ere, deduplikazio teknika aplikatuta duen datu biltegi batean ezin da *Verify* funtzioa burutu.

Gainera, deduplikazio teknika ondo aplikatzen ari zen probatzeko, beste segurtasun kopia oso bat programatu da. Lehengo segurtasun kopia osoak 109GBko pisua du eta konprimaketa teknika aplikatuta 86GB era murriztu da. Bigarren kopia oso honek, %98ko murrizketa sortu du eta ondorioz, soilik 1.31GBeko tamaina duen kopia sortu da, teknika ondo aplikatu dela bermatuz.

Segurtasun kopien egoera zuzena bermatu da, aste bateko jarraipena eta kontrola burutuz.

## **8. Segurtasun kopien berreskuratzea probatu**

Berreskuratze bat egiterako orduan, lehenik eta behin, informazioa ze egunetik aurrera berreskuratu nahi den jakin behar da eta ea hori burutzea posible den aztertzea. Kasu honetan, hilabete bat pasa bada, ezingo da aurreko hilabeteko egun zehatz baten segurtasun kopia berreskuratu, hala konfiguratu baitda, eta beraz, aukera bakarra hilabeteko azken ostiralean sortutako segurtasun kopia berreskuratzea da. Hilabetean bertan egun baten segurtasun kopia berreskuratu nahi bada, hori burutzeko aukera egongo da.

Bi motako berreskuratzeak probatu dira:

### **8.1. *Recovery Point* batetik fitxategi batzuen berreskuratzea**

Egunero sortzen diren segurtasun kopia inkrementalak *Recovery Point* (RP) bat sortzen dute, beraz, astelehenetik-ostiralera bitarteko margen horretako edozein egunetik berreskuratu daiteke informazioa. Bi proba egin dira:

- Segurtasun kopia osoko RPetik berreskuratu “Recovery Test” izeneko karpeta.
- Ostiralean sortutako segurtasun kopia inkremental baten RPetik berreskuratu “Recovery Test” izeneko karpeta.

Proba hau lehenengo kasua azkarragoa izango dela bigarrena baino egiaztatzeko burutu da.

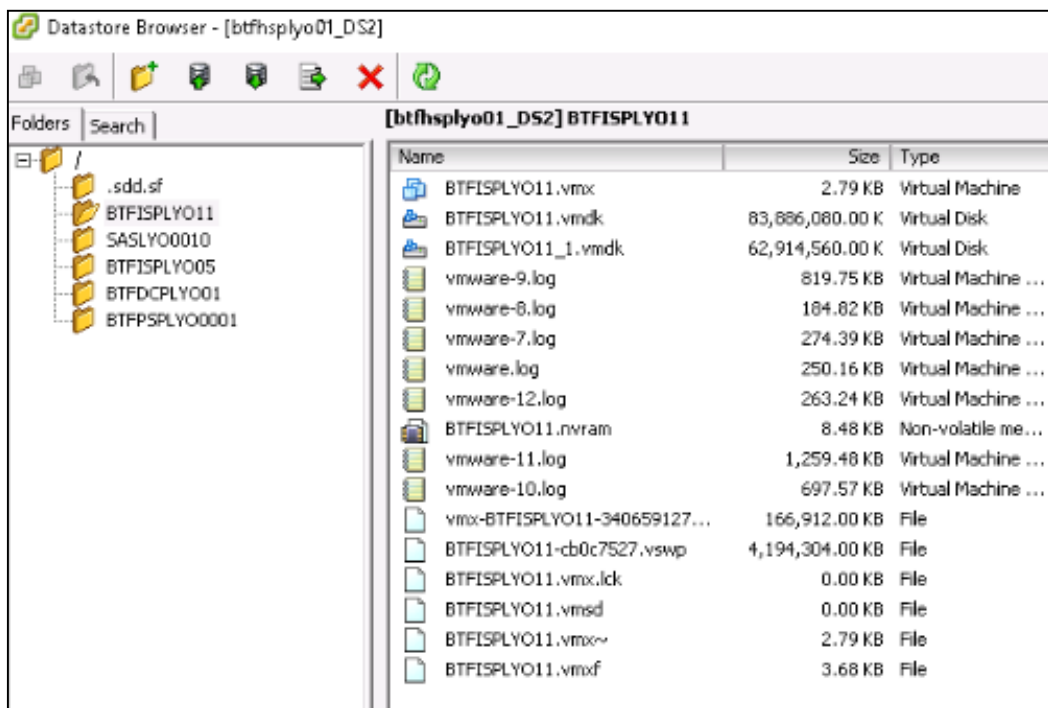
Horretarako hainbat fitxategiz osatutako “Recovery Test” izeneko karpeta bat sortu da BTFISPLYO11 zerbitzarian. Horren segurtasun kopia burutu ondoren, karpeta hori ezabatu egin da. Segurtasun kopia berreskuratzerako orduan, segurtasun kopia osoak sortutako RPetik soilik ezabatu den karpeta aukeratu da hori berrezartzeko. Prozesua zuzen burutu da, 1,6GBeko datuak berreskuratuz 2 segundotan.

Bigarren kasuan prozedura berdina erabili da, baina kasu honetan emaitzak desberdinak izan dira, berreskuratze denbora segundo batean handituz. Kasu honetan, distantzia oso txikia da baina geroz eta tamaina handiagoko berreskuratze bat egin, geroz eta diferentzia handiagoak egongo dira bi prozedura hauen artean. Izan ere, 3.4. atalean aipatu den bezala, azken kopia osoa eta ondorengo kopia inkremental guztiak berreskuratu behar dira nahi den egunaren kopiaraino iritsi arte.

## 8.2. Makina baten berreskuratze osoa

Arazo asko direla medio, gerta daiteke makina oso bat berreskuratzeko beharra izatea. Kasu hau burutzeko, beste zerbitzari batekin probatu da, zehazki, BTFISPLYO11 zerbitzariarekin, tamaina txikia duen zerbitzaria delako.

RP batetik makina birtual oso bat berreskuratzeko, beste plan bat konfiguratzeko beharrezkoa da segurtasun kopiak agente gabe burutzeko. Hala egin behar da, izan ere, agentearekin burututako kopiak makina birtual horretako diskoen kopia burutzen duelako fitxategi mailan. Agenterik gabe burututako kopiak ordea, makina birtual horren baliabide guztiak gordetzen ditu, konfigurazio fitxategiak, diskoak, etab. Hobeto ulertzeko jarraian agertzen den 5.3. irudian, makina birtual bat osatzen duten fitxategiak agertzen dira.



5.3. irudia. VMware ESXi zerbitzari baten egitura.

Azpiegitura hau, VMware ESXi zerbitzari batek osatzen du non horrek beste makina birtual batzuen kontrola duen, kasu honetan, erroa izanik. Erroan dagoen zerbitzari hori berezia da, izan ere ez da makina birtual normal bat, sistema eragile bezala VMware ESXi duelako. Zuhaitz horretako nodo bat berreskuratzea da helburua, zehazki BTFISPLYO11 zerbitzaria.

Kasu honetan, zerbitzari hau bi diskoz osatuta dago (“BTFISPLYO11.vmdk” eta “BTFISPLYO11\_1.vmdk”) eta agentea bertan instalatuko da. Ondorioz, soilik diskoan bertan dauden fitxategiak gordeko dira. Agenterik gabeko kopian aldiz, irudian agertzen diren fitxategi guztiak kopiatuko litzatezke, hau da, konfigurazio fitxategi guztiak.

Beraz, agenterik gabeko segurtasun kopia beharrezkoa da, makina birtual baten berreskuratze osoa burutzeko. Hala egiten ez bada beste aukera bat, makina birtual bat hasieratik sortzea izango litzateke, erabiltzaileak konfigurazio berdinak ezarriz eta ondoren diskoan dauden

fitxategiak inportatuz. Kasu horretan, arazoak egon daitezke, konfigurazioren bat kointziditzen ez baduelako erroreak egon daitezkeelako. Berreskuratzerako orduan, BTFISPLYO11 zerbitzaria ordezkatu beharrean beste bat sortu da izen desberdin batekin, BTFISPLYO11\_TEST eta *VMware ESXi* zerbitzariaren barne. Azkenik, zerbitzari berri hau lista honetan gehitu da.

## 5.2 Fase finala

Fase honetan LYO egoitza osoa babesteko eta beste egoitza bateko zerbitzari bat babesteko planifikatu den konfigurazioa azalduko da. Kasu honetan, aurrekoan ez bezala, zerbitzari gehiago daudenez, plan desberdinak sortu dira bakoitzari dagozkien beharrak zehaztuz. 5.1. taulan sortu diren planen laburpen bat azaltzen da.

Plana	Nodoak	OS	Babestutako unitateak	Egutegia
1	BTFISPLYO05 BTFISPLYO11 BTFDCPLYO01 BTFISPLYO01	WIN	Guztiak	➤ <b>Inkrementala</b> (23) Astelehenetik-Ostiralera ➤ <b>Osoa</b> (24) Hilabeteko azken ostirala
2	BTFFSPLYO01	WIN	D:\ unitateko zenbait karpeta	➤ <b>Inkrementala</b> (552) Astelehenetik-Ostiralera
3	BTFISDDTC01	WIN	Guztiak	➤ <b>Inkrementala</b> (552) Astelehenetik-Ostiralera
4	Btfasplynex1	Linux	Guztiak	➤ <b>Inkrementala</b> (23) Astelehenetik-Ostiralera ➤ <b>Osoa</b> (24) Hilabeteko azken ostirala

5.1. taula. Fase finalaren planen ezaugarriak.

Lehenik eta behin, nodo guztiak, kontsolara gehitu dira. Aurreko fasean sortutako datu biltegi eta RPS berbera erabiliz, deduplikazioaren eta konprimaketaren abantailak aprobetxatuz. Kasu honetan, lau plan ezberdin sortu dira, sistema eragilearen, kokalekuaren eta babestu behar diren unitateen arabera bereiztuz.

Lehenengo planari dagokionez, proba fasean sortutako plan berbera da, aurreko atalean azaldutako *Verify* funtziorik gabe eta nodo gehiago gehituz. BTFDCPLYO01 eta BTFISPLYO01 zerbitzarien kasuan, soilik *System State*, DCren artxiboen eta DCHParen *scope*-aren segurtasun kopia burutzea beharrezkoa da, beraz, ez litzateke beharrezkoa kopia osoa egitea. Arazoa zera da, DCren eta DCHPren konfigurazioa fitxategiak lortzeko *script* bat programatzea beharrezkoa izango litzatekeela haien konfigurazioa esportatzeko, eta ondoren honen segurtasun kopia burutzea. Prozesu horren abantaila, soilik beharrezkoak diren fitxategien segurtasun kopia burutzen dela da, tamaina murriztuz. Desabantaila aldiz, hondamendi baten aurrean, zerbitzaria berrezartzerako orduan denbora gehiago beharko duela da, RTO parametroa handituz.

Kasu honetan, bi zerbitzari hauen unitate guztien tamaina baxua denez (20GB eta 17.5GB) zerbitzari guztiaren segurtasun kopia egitea erabaki da, berreskuratzerako orduan aplikazio kritikoak direnez azkarrago berrezarri daitezkeelako.

Bigarren planari dagokionez, BTFFSPLYO01 nodoa, fitxategien zerbitzari bat denez, soilik D:\ unitatea babestuko da, hondamendi baten aurrean, helburu nagusia fitxategiak errekuaratzea izango delako eta ez zerbitzari guztia zegoen bezala uztea. C:\ unitateak sistema eragilearen informazioa gordetzen duenez, honen segurtasun kopia ez egitea erabaki da, beharrezkoa ez delako.

Beste planekin alderatuz, egutegi desberdin bat planifikatu zaio. Tamaina handiko unitatea (3TB) babestu behar denez, segurtasun kopia osoa burutuko da eta hortik aurrerako *Backup* guztiak inkrementalak izango dira, bi urteko erretentzioa izanik. Hilabete batek gehienez 23 lan egun ditu, beraz, kopiak bi urtez gorde nahi direnez, 24 hilabetez gorde beharko dira, hau da, 552 kopia gehienez egin beharko dira. Horri esker, hilerok, ez da segurtasun kopia osoa gorde beharko, ondorioz, kopia inkrementalak tamaina txikiagoa behar dutenez, diskoaren espazio librea handiagoa izango da.

Plana aurrera eramaterakoan arazoak egon dira. Diskoaren tamaina 2TBkoa denez eta BTFFSPLYO01 zerbitzariaren D:/ unitateak oraingoz 3TBko tamaina (denbora pasa ahala tamaina handituko da) duenez, ezinezkoa izango da LYO egoitzako zerbitzari guztien segurtasun kopiak gordetzea datu-biltegi berdinean nahiz eta, konprimaketa eta deduplikazio teknikak erabili.

Arazo horri aurre egiteko, bi soluzio berri pentsatu dira. Batetik, D:/ unitateko fitxategi espezifikoko kopiak, ondorioz, zenbait fitxategi baztertuz eta eraginkortasuna galduz. Bestetik, RPS birtual bat sortzea LYO egoitzan eta ondorioz, datu-biltegi handiago bat sortu soilik, zerbitzari honen segurtasun kopiak gordetzeko. Lehenengo irtenbidea burutzeko, programatutako planean, karpeta espezifikoen *path*-a sartu beharko da. Ondoren, programak, fitxategien kokalekua nodo berri bat bezala identifikatuko du, bakoitzari plan bat esleituz.

Bigarren aukera aurrera eramateko ordea, RPS berri bat sortu beharko da eta bertan datu-biltegi berdina. Azkenik, plan berri bat sortu, datu biltegi berriaren kokalekua adieraziz.

Hirugarren planari dagokionez, beste egoitza batean kokatzen den zerbitzari bat babestu behar da. Kasu honetan, prozesua motelagoa izango da, LYO egoitzako LAN saretik irten behar duelako MPLS tik pasa eta DTC iristeko. Hori dela eta, inkrementalez osatutako plana planifikatu da, datu kopuru txikia garraiatzeko MPLS saretik zehar.

Azkeneko planari dagokionez, ezin izan da burutu, Linux nodoak kontsolara gehitzeko Linux *Backup* zerbitzari bat beharrezkoa delako. Gaur egun, enpresak ez du zerbitzari hori sortzeko intentziorik, beraz, Linux nodoak, software zaharrarekin (*Arcserve Backup*) babestu dira.

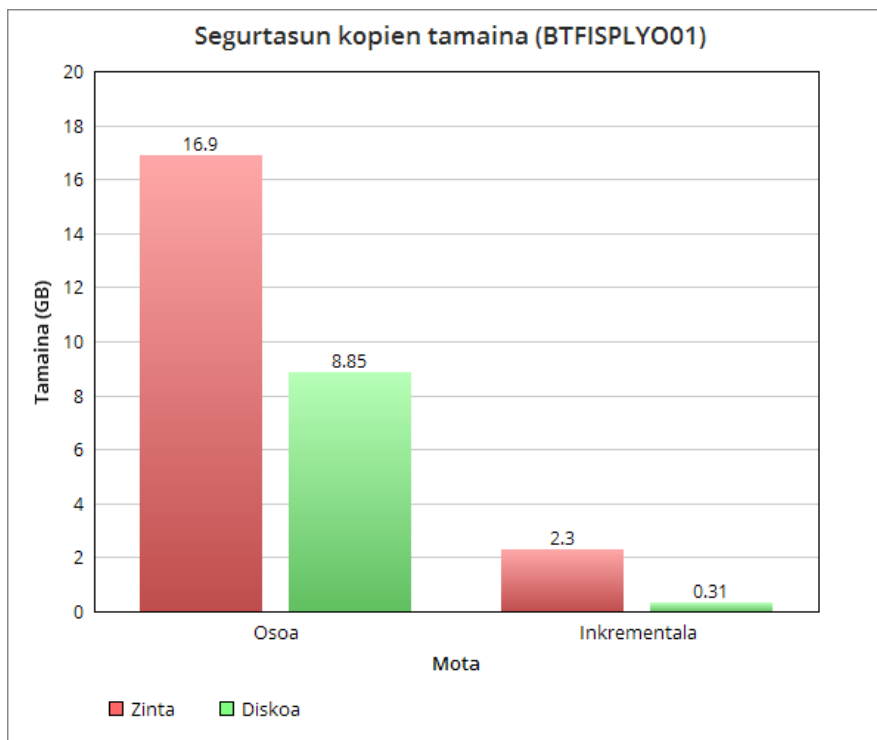
### 5.3 Emaizten analisia

---

Atal honetan, lortutako emaitzen arteko konparaketa azalduko da. Lortutako emaitzak, diskoan gordetako *Backup*-ak, *Arcserve UDP* programatik eta zintan gordetako *Backup*-ak *Arcserve Backup* programatik atera dira, bi motatako emaitzak lortuz:

- Segurtasun kopien tamainaren arteko konparaketa biltegiatze gailuaren arabera (zinta edo diskoa) eta motaren arabera (osoa edo inkrementala).
- Aste bateko tamainaren eboluzioaren grafikoa biltegiatze gailuaren arabera (zinta edo diskoa).
- Segurtasun kopiak burutzeko behar den denboraren arteko konparaketa biltegiatze gailuaren arabera (zinta edo diskoa) eta motaren arabera (osoa edo inkrementala).

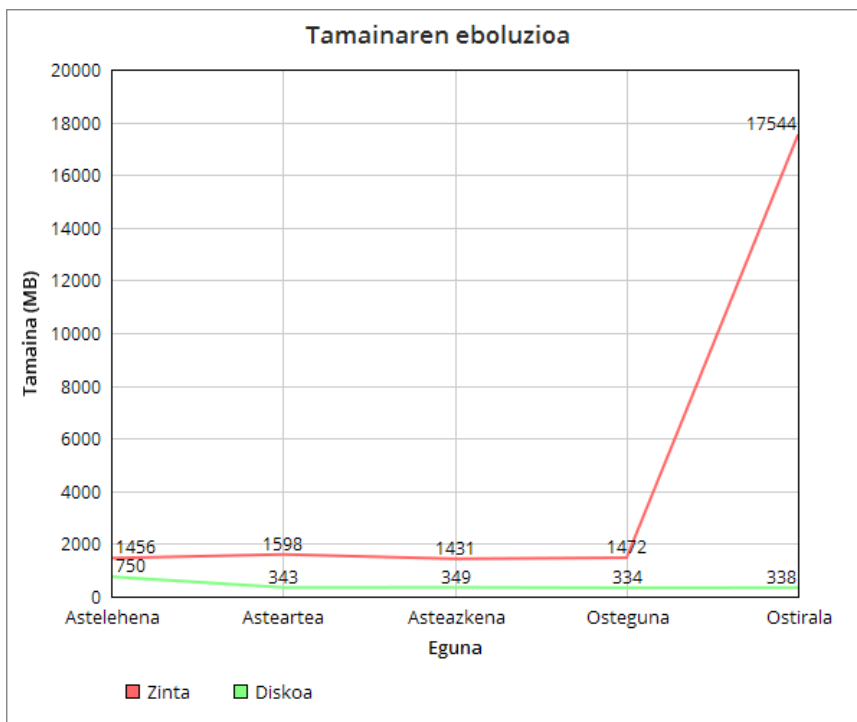
BTFISPLYO01 zerbitzaria erreferentzia bezala hartu da datuen analisia burutzeko. Zerbitzari honen tamaina totala 17,5GBkoa da, unitate guztiak batuta. 5.4. irudian, diskoaren eta zintaren arteko segurtasun kopien tamainak konparatuko dira.



5.4. irudia. Segurtasun kopien tamainen arteko konparaketa.

Bi motatako segurtasun kopiak alderatu dira, batetik, segurtasun kopia osoa eta bestetik, inkrementala. Bi kasuetan, ikusten da diskoan burutu diren *Backup*-en tamaina zintan burutzen direnekin alderatuta, nahiko txikiagoa dela. Diskoaren abantailetakoa bat erredukzio teknikak aplikatzen direla da, kasu honetan, deduplikazio eta konpresio teknikak. 5.3. irudian argi islatzen dira hauen efektua, zenbait kasutan, tamaina erdia baina gehiago murriztuz. Aipatu beharra dago, diskoan burutu den segurtasun kopia osoa, zerbitzari horretan burutu den lehenengo segurtasun kopia dela, hori dela eta, tamaina hori izango da maximoa. Hilabete bakoitzeko azken ostiralean egin behar den segurtasun kopia osoaren emaitzak ikusiz, askoz ere gehiago txikitu da segurtasun kopia oso honen tamaina, zehazki 0,3GBera murriztuz. Aldatu diren datuak gutxi izan direnez eta deduplikazio teknikari esker berriro ere sistema guztiaren datuak ez direnez errepikatu behar, asko murrizten da tamainaren faktorea.

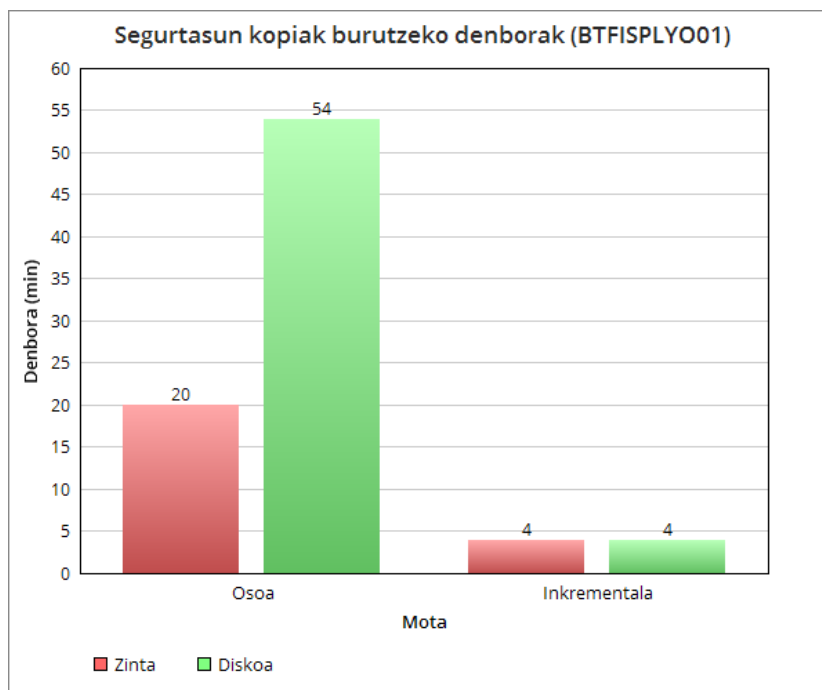
5.5. irudian ikusi daiteke aste bateko tamainaren eboluzioa:



5.5. irudia. Tamainaren eboluzioa.

Asteaz zehar burutzen diren segurtasun kopia inkrementalak tamaina txikiagokoak dira diskoan. Gainera ostiralero zintan segurtasun kopia osoa exekutatzenez, tamaina diferentzia asko handitzen da.

Oraingoan, segurtasun kopiak burutzeko denborak alderatu dira.



5.6. irudia. Segurtasun kopien denboren arteko konparaketa.



5.6. irudian ikusten denez, segurtasun kopia osoa burutzeko denbora askoz ere handiago izan da diskoaren kasuan, eta hori harritzekoa izan da. Aipatu den bezala, zerbitzari honen lehenengo segurtasun kopia da, hori dela eta, deduplikazio teknika aplikatuz, datu bloke bakoitzeko dauden datu blokeekin egin behar den konparaketa prozesuak luzatu du. B Eranskina atalean agertzen den bezala, hurrengo segurtasun kopia osoa egin denean, denbora hori murriztu egin da 8 minutu eta 51 segundotara pasatuz. Inkrementalaren kasuan, denbora berdina izan da.

Diskoaren beste abantailetakoa bat zintarenarekin alderatuta haren abiadura azkarra da. Kasu honetan, hori ez da grafikoan islatzen. Arazoa zerbitzaria eta biltegitratze gailuen arteko konexioa da. Zintaren kasuan, zerbitzari eta *tape library* arteko konexioa, SAS baten bidez denez, honen abiadura 6 GB/s-koa da. Diskoaren kasuan aldiz, konexioaren banda zabalera 100 MB/s-koa da, abiadura asko murriztuz.

Esan beharra dago, atal honetan agertzen diren emaitzak sare bereko, hau da, LYOeko LAN sarera konektatuta dauden zerbitzarien segurtasun kopien emaitzak direla. Beste egoitza bateko eta LYOko datu biltegian gordetzen diren segurtasun kopiak askoz ere denbora gehiago daramatzate, informazioa MPLS saretik garraiatu behar delako. Adibidez, 41GBeko tamaina duen segurtasun kopia oso bat egiteko 5 ordu eta 40 minutu behar izan dira. Inkrementalaren kasuan, 1.4 GBeko tamaina duen kopia 20 minututan burutu da, zenbait kasutan LAN sarean exekututzen direnarekin alderatuta 10 aldiz gehiago iraunduz.

Emaitza hauen analisi orokor bat eginez, segurtasun kopiak diskoan egitearen abantailak txikitu egin dira. Izan ere, zerbitzari baten lehenengo segurtasun kopiak egiteko denbora askoz handiagoa da zintan egiten denarekin alderatuta. Hortik aurrerako segurtasun kopia osoak egitean aldiz, azkarragoak dira, baina soilik datu gutxiago kopiatu behar direlako. Inkrementalen kasuan, antzeko denbora irauten dute.

Horretaz aparte, geratzen diren abantailak onak dira, batez ere tamainaren faktorea asko murrizten delako, kasu batzuetan %98ko murriztapena sortuz. Biltegitratze tamaina falta beti izan da arazoa, hori dela eta, diskoa erabiliz arazo hau ekidingo da. Gainera, metodo honi esker ez da beharrezkoa zintan ordezkapena, beraz, ez dago pertsonen interakziorik. Beste abantailetakoa bat, biltegitratze kokapena aldatzeko erraztasuna da, adibidez, biltegitratze handiagoa duen kokapen batera aldatuz.

Kopiak garatzeko softwarea (*Arcserve UDP*) ere eraginkorragoa da, kontsola intuitibo eta erraz bat erabiliz, monitorizazio zehatzago batekin eta estatistikak eta datuak lortzeko kapazidade handiarekin.

Neurtu diren emaitzak kontsultatu nahi badira, B Eranskina atalean aurkituko dira.

## 5.4 Script-en programazioa

---

Atal honetan, garatu diren *script*-ei buruzko informazioa agertuko da. Lehenik eta behin, 1.2.2. atalean azaldu bezala, segurtasun kopien egoera eta informazioa gordetzen duen prozesu automatikoa programatu da. Garatutako *script*-ak *Powershell ISE* bitartez programatu dira.

Gaur egun enpresako talde batek, egunero segurtasun kopiak burutzeko erabiltzen diren programa guztiak analizatzen ditu, segurtasun kopien egoera aztertuz. Egoeraren arabera, *Excel* fitxategi batean apuntatzen da, ondoren, beste ekipo batek hori aztertzeko eta konpontzeko. *Script* honen helburua prozesu hau saihestea da, errore-tasa murriztuz eta prozesu hau automatizatuz.

Horretarako, *script* honek egingo duena zera da: Erabiltzen diren segurtasun kopiak burutzeko bi programen (*Arcserve Backup* eta *Veeam*) datu baseetatik lortzen du beharko den informazioa. Behar diren datu guztiak beste datu baseko formatu ezberdin bateko taula ezberdinetan gordetzen dira, zehazki GLPIko datu basean, hau da, inbentarioa dagoen zerbitzarian hain zuzen ere. Ondoren *Power BI* aplikazioaz baliatuz, datu base honetara konektatuz, datuak era automatiko eta kontrolatu batean ikusteko aukera izango da, segurtasun kopien egoera aztertuz. Gainera finkatutako data batean (egunero, astero, etab.) segurtasun kopiei buruzko informazioa ikusteko aukera egongo da.

*Arcserve Backup* programarentzat *script*-a lehendik sortua izan da. Hori dela eta, kasu honetan, *Veeam* programarentzat burutu da prozesua. Ondoren bi programa hauen datuak elkartuko dira aipatutako GLPIko datu basean. *Script*-a garatzeko programatu den kode guztia errepositorio honetan aurki daiteke: “ <https://github.com/molla97/Scriptaren-kodea> ”

Lehenik eta behin, datu basea atzitzen eta kontsulta bat itzultzen duen “*DBQuery.ps1*” *script*-a garatu da, bi motatako datu baseentzako (SQL eta MySQL). *Script*-a bi funtzioak osatzen dute:

### 1. Sql-QueryDB

```
function Sql-QueryDB {  
  
    #Parametroak  
  
    param([string]$sqlHost = $null, [string]$sqlInstance = $null,  
        [string]$sqlDBName = $null, [string]$sqlQuery = "")
```

5.1. kodea. Sql-QueryDB funtzioaren definizioa.

Funtzioa 5.1. kodean ikusten den bezala, lau parametroz osatuta dago, guztiak `string` motakoak:

- `sqlHost` : SQL zerbitzariaren izena.
- `sqlInstance` : Datu basearen instantziaren izena.
- `sqlDBName` : Datu basearen izena.
- `sqlQuery` : Sortutako kontsulta kodea.

Ondoren, 5.2. kodean hiru konprobaketa egiten dira parametroak hutsak ez direla egiaztatzeko. Kasuren batean hutsa edo null bada, errore mezua azalduko da zein parametro den adieraziz.

```
$sqlConnection = New-Object System.Data.SqlClient.SqlConnection

    $sqlConnection.ConnectionString = "Server = $sqlHost\$sqlInstance;
Database = $sqlDBName; Integrated Security = True; Connect Timeout=30;
ApplicationIntent=ReadOnly; Pooling=true"

    $sqlCmd = New-Object System.Data.SqlClient.SqlCommand

    $sqlCmd.CommandText = $sqlQuery

    $sqlCmd.Connection = $sqlConnection

    $sqlAdapter = New-Object System.Data.SqlClient.SqlDataAdapter

    $sqlAdapter.SelectCommand = $sqlCmd

    $dataSet = New-Object System.Data.DataSet

    $sqlAdapter.Fill($dataSet)
```

5.2. kodea. Datu basearen konexioa.

Azkeneko pausoa eta garrantzitsuena, datu basearekin konexioa ezartzea da. Horretarako `SqlConnection` objektua sortu behar da, honek datuen SQL zerbitzari baten sesioa errepresentatzen du. Honekin batera, `SqlDataAdapter` eta `SqlCommand` erabiltzen dira errendimendua handituz. `Fill` metodoari esker, datuak pasatzen dira objektu batetik bestera. Bukatzeko, parametroak berrezartzen dira eta `dataSet` objektua itzultzen da.

## 2. MySql-QueryDB

Beste funtzioan bezala parametroak definitzen dira, kasu honetan hiru dira:

- `sqlHost` : SQL zerbitzariaren izena.
- `sqlDBName` : Datu basearen izena.
- `sqlQuery` : Sortutako kontsulta kodea.

Bukatzeko konexioa ezartzen da datu basearekin.

Jarraitzeko, *Veeam* programaren datu basetik informazioa berreskuratzen duen **“getVeeamJobs.ps1”** *script*-a garatu da. Bertan `veeam-getJobs` funtzio bakar bat garatu da. Honek, exekutatu diren segurtasun kopiei buruzko informazioa lortzen du, adibidez, exekutatu den zerbitzaria, data, egoera, etab.

Funtzio honek 6 parametro jasotzen ditu, baina funtzioa exekutatu ahal izateko bakarra da beharrezkoa. Hau kontrolatzeko `mandatory` parametroaz baliatu da:

- paramSqlHost : Segurtasun kopiak burutzen dituen programaren datu basea dagoen zerbitzariaren izena.
- paramSqlInstance : Datu basearen instantziaren izena.
- paramHostName : Backup zerbitzariaren izena
- paramEndDate : SQL kontsultaren parametro bat definitzeko erabiltzen den parametro boolearra.
- paramBefore : Data bat baino lehen sortutako segurtasun kopiak filtratzeko parametroa.
- paramAfter : Data baten ondoren sortutako segurtasun kopiak filtratzeko parametroa.

```

$sqlQuery = "SELECT
            T2.id AS 'jobId',
            job_name AS 'jobName',
            T1.description AS 'jobDescription',
            result AS 'jobResult',
            job_type AS 'jobType',
            modified_by AS 'jobOwner',
            creation_time AS 'jobCreationTime',
            end_time AS 'jobEndTime',
            CASE
                WHEN creation_time > end_time THEN NULL
            ELSE
                CONVERT (VARCHAR, DATEADD (minute,
DATEDIFF(minute, creation_time, end_time), 0), 8) END AS 'jobWallTime'

            FROM [VeeamBackup].[dbo].[BJobs] T1
            INNER JOIN
            [VeeamBackup].[dbo].[Backup.Model.JobSessions] T2 ON
            T1.id=T2.job_id
            WHERE job_name LIKE '%00%-%'
            $sqlWhereJobsDate
            ORDER BY creation_time DESC"

$jobs = Sql-QueryDB -sqlHost $paramSqlHost -sqlInstance
$paramSqlInstance -sqlDBName $sqlDBName -sqlQuery $sqlQuery

```

5.3. kodea. SQL kontsulta.

Ondoren zenbait parametro hasieratzen dira eta existitzen diren plan guztiak eskuratzen dira, SQL kontsulta bati esker (5.3. kodea), kasu honetan, planak jobs parametroa bidez adierazten dira. Kontsulta hau parametro bezala pasatzen da lehenago komentatutako datu basera konektatzeko funtzioari (Sql-QueryDB). Jarraian, aurkitutako plan guztiei zenbait konprobaketa aplikatzen zaizkio eta abisu mezuz guztiak message parametroan gordetzen dira. Plan kopuruek muga bat (lehenago definitutako parametroa) gainditzen badute, hala adierazten duen mezua gordeko da, bestela aurkitutako plan kopuru totala gordeko da. Azkenik, planik aurkitu ez bada, hala adieraziko da message parametroan.

Ondoren, "job" bakoitza, hau da, datu basean aurkitutako plan bakoitza hash-taula batean gordeko da (jobArray), plan bakoitzeko hainbat informazio gordez, bere ID-a, izena, data, etab.

Prozesu berdina aplikatuko da sesioentzako eta baita log-entzako. Sesioen kasuan, beste hash-taula bat sortuko da, sessionArray izenarekin. Kasu honetan ere, informazio gehiago gordeko da. Log-en kasuan aldiz, zuzenean jobArray hash-taulan gordeko dira.

```

$sessionsArray.add($sessionsArray.Count, $sessionArray)

#Add sessions to job table
$jobArray.add("sessions", $sessionsArray)

#Add job table to jobs table
$jobsArray.add($jobsArray.Count, $jobArray)

#Return values init
$returnArray.add("hostName", $paramHostname)
$returnArray.add("message", $message)
$returnArray.add("jobs", $jobsArray)

Return $returnArray

```

5.4. kodea. Informazioa dagokion Hash-taulan txertatzea.

5.4. kodean ikusten den bezala sesio guztiak `sessionsArray` hash-taulan gorde dira ondoren hauek `jobArray`-ean txertatzeko. Beraz, "job" bat hainbat sesioez eta hainbat log-ez osatuta dago. Bukatzeko, `returnArray` hash-taula itzultzen da, bertan, *backup* zerbitzariaren izena, aurreko pausotan egindako konbrotaketen ondoren sortutako mezua eta "job"-ak aurkitzen diren.

Adibidez, "24/06/2019 00:00:00" baino beranduago bukatu diren segurtasun kopien informazioa berreskuratzeko, `Veeam-getJobs` funtzioari deituz 5.7. irudian agertzen den emaitza lortuko da:

Name	Value
message	29 jobs has been found.
hostName	SISDTC0051
jobs	{28, 27, 26, 25...}

5.7.irudia. Veeam-getJobs funtzioaren adibidea.

Azkenik, "ApplInterface.ps1" *script*-a garatu da. Programa hori bost funtziok osatzen dute, non helburu nagusia, *Arcserve Backup* eta *Veeam* programen segurtasun kopien informazioa berreskuratzea eta datu base berriak txertatzea da. Datu base berriak MYSQL sistema erabiltzen du eta lau taulez osatuta dago. Lehenengoak, *backup* zerbitzariaren izena eta segurtasun kopiak burutzeko instalatuta dagoen softwarearen izena gordetzen du. Bigarrenak ordea, job-ei buruzko informazioa gordetzen du. Hirugarrenak, log-ei buruzko informazioa eta azkenik, laugarrenak, sesioei buruzko informazioa. Honako hauek dira azken *script*-a osatzen dituzten funtzioak:

#### 1. BackupReport-fullExtraction

Lehenik eta behin, `$backupHosts` aldagaian existitzen diren *backup* zerbitzariak gordetzen dira, SQL kontsulta bat burutuz. Prozesu berdina jarraitzen da, "job"-en ID-ak berreskuratzeko, kasu honetan, `$data` aldagaian gordez.

```

if ($data.Tables[0].Rows.bkpjob_id.count -eq 0)
{
    echo ("DB empty")
    $dte = Get-Date
    $getJobAfterDate= $dte.AddDays (-365)
}
else
{
    echo ("DB Information")
    $dte = Get-Date
    $getJobAfterDate= $dte.AddDays (-1)
}

```

5.5. kodea. Datu basearen informazioa egiaztatu.

5.5. kodean, datu basea ea hutsa dagoen edo ez egiaztatzen da. Hutsa badago azken 12 hilabeteetan sortu diren *Backup* guztien informazioa berreskuratuko da.

Datu basean, daturen bat badago ordea, exekutatu den eguna baino egun bat lehenagotik sortu diren segurtasun kopia guztien informazioa, soilik, berreskuratuko da. Honi esker, *script*-a automatikoki exekutatzeko aukera sortu da. Gainera, ez-ustekabe batean, datu basea ezabatzen bada, automatikoki berriro beteko da, orain burututako egiaztapenari esker.

Jarraian, zerbitzari bakoitzeko, instalatuta duen softwarearen arabera (*Veeam* edo *Arcserve Backup*) *Softwarearen\_izena-extractForBackupReport* funtzioari deitzen zaio "job"-ak eskuratzeko.

"Job" bakoitzeko, *BackupReport-insertData Softwarearen\_izena* funtzioari deitzen zaio, informazioa dagoen datu base berriko tauletan txertatzeko.

## 2. *BackupReport-insertDataSoftwarearen\_izena*

Horrelako bi funtzio existitzen dira, software bakoitzeko bat. Horri esker, "job" bakoitzaren datuak dagozkion tauletan txertatzen dira. Esan beharra dago, taula hauen formatua finkatuta dagoela, ondorioz, informazioa eskuratu ez den aldagaietan, *null* balioa ipini da.

## 3. *Softwarearen\_izena-extractForBackupReport*

Horrelako bi funtzio existitzen dira, software bakoitzeko bat. Funtzio honen eginkizun bakarra "job"-en informazioa eskuratzea da. Horretarako, aurreko *script*-ean sortutako *Veeam-getJobs* edo *Arcserve-getJobs* funtzioari deitzen zaio parametroak finkatuz.

Bukatzeko, funtzio eta *script*-ak probatzeko *TEST.ps1 script*-a erabili da.

Laburbilduz, programatutakoari esker, segurtasun kopien software ezberdinen datuak gorde daitezke datu base berdinean. *Script*-a egunero automatikoki exekutatzeko programatu da, Windowseko ataza programatzaileari esker.

Ondoren, datu base horretara konektatuz, *Power BI* aplikazioa erabiliz, prozesua automatizatu eta estandarizatu da.

The screenshot shows a backup management interface. At the top, there's a date range from 16/06/2019 to 01/07/2019. Below that is a calendar grid where each cell represents a backup job's status for a specific day. The jobs listed include '002 - Backup WIN MSSQL - C3', '004 - Backup ASP - C3', '005 - Backup MSSQL ASP - C2', '006 - Backup ALL - C1', '007 - Backup HOM/TEST/DEV', 'Backup Configuration Job', 'Backup LYO', 'Backup ORE', 'Backup RUE', 'Backup VEN', and 'TEST - Auto Backup Report'. The status colors range from green (Finished) to red (Failed) and yellow (Warning).

Below the calendar is a detailed log table with the following columns: Host, Path, Status, Elapsed Time, Backup dFile, MissedFile, Backup dDataMB, Date Start, log\_LogTime, and bkpllog\_msgtxt.

Host	Path	Status	Elapsed Time	Backup dFile	MissedFile	Backup dDataMB	Date Start	log_LogTime	bkpllog_msgtxt
BTDFCPLYO01	WMI Writer	Finished	0:00:00	8	0	39,61	28/06/2019 16:04:22	06/2019 23:53:02	Backup Operation Successful.
BTDFCP RUE01	WMI Writer	Finished	0:00:00	8	0	46,05	17/06/2019 22:06:40	06/2019 6:07:13	Backup Operation Successful.
BTDFCP RUE01	WMI Writer	Finished	0:00:00	8	0	46,05	18/06/2019 22:09:54	06/2019 18:00:11	Backup Operation Successful.
BTDFCP RUE01	WMI Writer	Finished	0:00:00	8	0	46,05	21/06/2019 22:20:10	06/2019 3:23:59	Creating VM snapshot
BTDFCP RUE01	WMI Writer	Finished	0:00:00	8	0	46,05	26/06/2019 22:12:06	06/2019 3:24:54	Creating VM snapshot
BTDFCP RUE01	WMI Writer	Finished	0:00:00	8	0	46,05	28/06/2019 22:17:54	06/2019 5:13:32	Creating VM snapshot
BTDFCP RUE01	WMI Writer	Finished	0:00:00	8	0	46,05	28/06/2019 22:17:54	06/2019 6:27:41	Creating VM snapshot
BTDFSPLYO01	D:\Appl\Arcserve\ARCserve Backup\DRBTDFSPLYO01\BTDFCPLYO01	Finished	0:00:00	30	0	0,35	17/06/2019 22:35:12	06/2019 11:53:47	Creating VM snapshot
								06/2019 11:53:48	Creating VM snapshot
								06/2019 11:54:43	Creating VM snapshot
								06/2019 11:54:43	Creating VM snapshot
								06/2019 20:23:41	Creating VM snapshot
<b>Total</b>				<b>70511614</b>	<b>28</b>	<b>381.988.943,97</b>			

5.8. irudia. PowerBI programa bitartez sortutako automatizazioa.

5.8. irudian ikusten den bezala, automatizazioa hiru taulek osatzen dute, dataren arabera filtratzeko aukera izanik:

1. Oinarrizko Taula: Goialdean eta erdian kokatuta dagoen taula da. Exekutatu diren "Job" guztiak agertzen dira dataren arabera sailkatuta. "Job"-a osatzen duten sesioen batek huts egiten badu, gorri agertuko da. Exekuzioan zehar "Warning"-ren bat badago, horiz agertuko da. Azkenik, dena ondo burutu bada, berdez agertuko da.
2. Sesioen Taula: Ezkerraldean eta behean kokatuta dagoen taula da. Bertan, oinarrizko taularen "Job" batean klik eginez gero, honek dituen sesio guztien informazioa agertuko da.
3. Log-en Taula: Eskuinaldean eta behean kokatuta dagoen taula da. Bertan sesioen taulan, sesio bati klik eginez gero, haren log-a agertuko da. *Veeam* programako sesio bat bada eta ondo burutu bada, ez da log-ik agertuko, hala programatu baita.

Planifikatutako bigarren *script*-a ez da garatu, programa bera konfiguratu daitekeelako automatikoki kopiak burutzeko.

## 5.5 Aurrera eramateko proposamenak

---

Atal honetan proiektuaren hobekuntza proposamenak eta ideiak aipatuko dira, etorkizun batean aplikatu daitezkeenak.

### 1. *Arcserve UDP eta Arcserve Backup-en nahasketa (D2D + D2Tape)*

Proposamen hau LYO egoitzan erabiltzen diren segurtasun kopiak burutzeko bi metodoen nahasketan datza. Proiektua garatu aurretik, LYO egoitzan segurtasun kopiak gordetzeko zintak erabiltzen ziren. Orain aldiz, badaude zenbait zerbitzari, proiektu honetan konfiguratu direnak, zinta erabiltzeari utzi diotenak eta diskora pasa direnak. Bi metodoak konbinatu daitezke egoitzaren funtzionamendua hobetuz. Planifikazioa ondorengoa izango litzateke:

5.2. atalean aipatutako planifikazio berbera jarraitzea, baina kasu honetan, hilabetearen azkeneko ostiralean segurtasun kopia oso bat zintan gordetzea. Ekintza hau plan guztiei aplikatuko zaie. Diskoaren arazoa, zintarenarekin alderatuta, tamaina txikia eta prezio altua izan dira beti, hori dela eta, proposamen honekin diskoa hustuko litzateke hilabete bukaeran, berria izango balitz bezala utziz. Gainera, tamaina murrizketa teknikak aplikatzen direnez ez litzateke beharrezkoa disko baten biltegitratze tamaina handia. Kasu honetan diskoak 2TBeko tamaina du, baina disko txikiago bat ere onargarria izango litzateke. Abiadurari dagokionez, behin zerbitzari bakoitzaren lehengo kopia burututa azkarragoa edo berdina izango da. Esan beharra dago, gizakiaren interakzioa kasu honetan beharrezkoa izango dela, denbora periodo batean zinten aldaketa burutzeko.

Laburbilduz, proposamen honekin teknika zaharra baztertu ordez, teknika berrirabiltzen da, zintak aprobetxatuz. Metodo honekin beraz, biltegitratze tamaina, abiadura eta erretentzio denbora hobetuko dira.

### 2. **Segurtasun kopiak garatzeko metodologiaren aldaketa egoitza desberdinetan.**

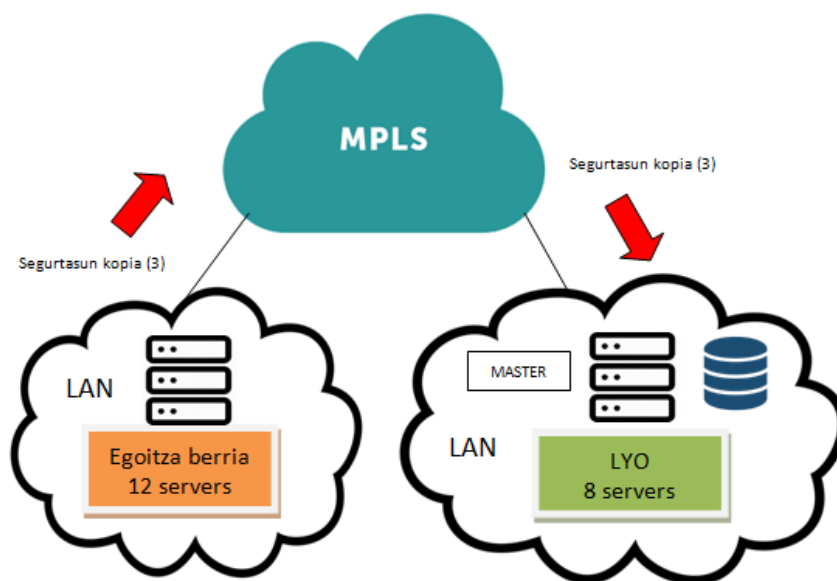
Egoitza guztien segurtasun kopia burutzeko programen zentralizazioa proposatzen da. Egoitza guztietan *Arcserve UDP* programa erabiltzea gomendatzen da. Biltegitratze gailu bezala zinta edo diskoa erabiltzeko aukera eskaintzen duenez, ez da bi erreminta desberdinen erabilera behar. Horrela, beste *software* baten ikaskuntza ez litzateke beharrezkoa, soilik planifikazio eta metodologia desberdina *software* berdinean.

### 3. **Egoitza guztietan datu biltegiak ezartzearen arkitekturaren ebaluazioa.**

Egoitza guztietan datu biltegi bat sortuko da, horrela informazioa ez da garraiatuko joan eta etorrian MPLS saretik egoitza batetik bestera, kontsola LYO egoitzan aurkitzen baitda. Gaur egun, datu biltegia kontsola instalatuta dagoen zerbitzarian bertan aurkitzen da, LYO egoitzan hain zuzen ere. Egoitz berdineko zerbitzarien segurtasun kopiak azkar burutuko dira LAN sarearen bitartez konektatuta daudelako baina beste



egoitzako kopiak egin behar badira aldez, MPLS saretik garraiatu beharko da informazioa, abiadura motelduz. Prozesua 5.9. irudian agertzen dena da:



5.9. irudia. Datu biltegia ez dagoen egoitza bateko segurtasun kopiaren prozesua.

1. Kontsolatik dagokion egoitzako sistemaren segurtasun kopiaren agindua exekutatzen da (LYO - Egoitza berria).
2. Egoitza horretako segurtasun kopia burutzen da (Egoitza berria).
3. Segurtasun kopia hori garraiatzen da datu biltegiraino (Egoitza berria - LYO).

Hala dela egiaztatzeko, DTCeko BTFISDDTC01 zerbitzariari segurtasun kopia bat programatu zaio LYOkoko datu biltegian gordeko dena. *Ntop* programaren bitartez, ikusi daiteke trafikoa dagoela DTCeko zerbitzari eta LYOkoko datu biltegiarekin, MPLS saretik zehar.

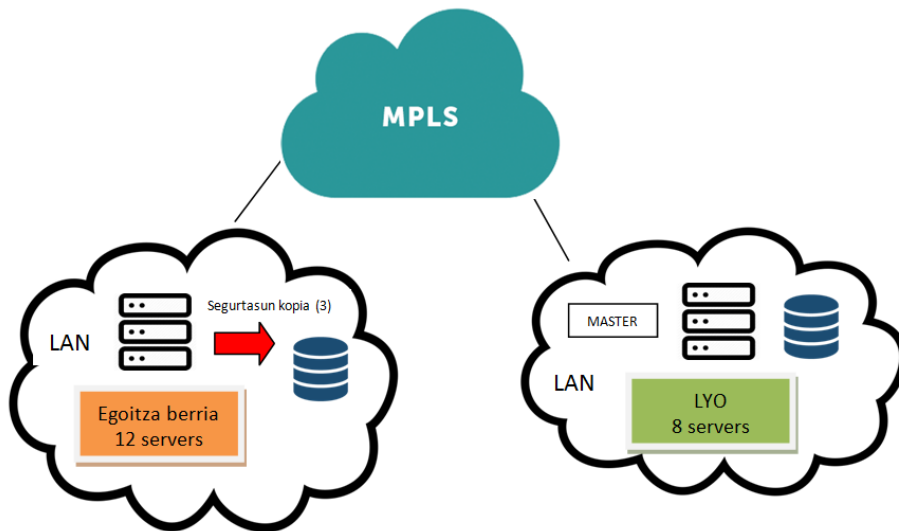
- LYO egoitzako datu biltegiaren zerbitzariaren IP helbidea 42.0.100.203 da.
- DTC egoitzaren BTFISDDTC01 zerbitzariaren IP helbidea 10.13.8.30 da.
- *Vmware ESXi* erro zerbitzariaren IP helbidea 10.16.10.51 da.

Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes
42.0.100.203 :microsoft-ds	BTFISPDTC05:52003	51:21	Client	649.2 kbit/s ↓	233.26 MB
42.0.100.203 :ms-wbt-server	BTFISPDTC06:64012	01:03:03	Client	23.17 kbit/s ↑	12.07 MB
42.0.100.203 :57732	BTFISPDTC05:microsoft-ds	06:47	Client	0 bit/s —	8.2 KB
42.0.100.203 :57517	10.16.10.51:ideafarm-door	11:21	Client Server	1.52 Mbit/s ↓	168.56 MB

5.10. irudia. DTC eta LYO arteko trafikoaren kontrola.

Lehenik eta behin, DTCeko zerbitzaria, *Vmware ESXi* erro zerbitzariarekin harremanetan jartzen da, ondoren, hau LYO egoitzako datu biltegiarekin harremanetan jartzeko 5.10. irudian ikusten den bezala.

Proposatutako arkitektura berria aplikatzen bada, prozesua desberdina izango da 5.11. irudian ikusten den bezala.



5.11. irudia. Egoitzetan datu biltegia dagoen segurtasun kopiaren prozesua.

Hirugarren pausoa informazioa MPLS bidez garraiatu ordez, LAN saretik garraiatuko da. Izan ere, egoitzan bertan izango du segurtasun kopia gordetzeko aukera, egoitza berriko datu biltegia hain zuzen ere. Hori dela eta, abiadura handituko da, segurtasun kopiak burutzeko denbora murriztuz.

Prozesu hau *Arcserve UDP* programan burutzeko, RPS berri bat sortu beharko da egoitza bakoitzean. Ez da beharrezkoa RPS-a zerbitzari fiskoa izatea, birtuala ere izan daiteke, horrela, datu biltegi handiago bat izateko aukera egongo da. Bukatzeko, egoitza guztietako RPS-an nahi diren datu biltegiak sortuko dira. Kasu honetan ikusten da segurtasun kopiaren trafikoa LAN sarean zehar garraiatzen dela eta ez MPLS tik zehar.

# 6

---

---

## Konparaketa

## 6.1 Softwarearen konparaketa

Atal honetan gaur egun segurtasun kopiak garatzeko eta sistemak babesteko merkatuan dauden bi programa garrantzitsuenetakoen arteko konparaketa burutuko da. Lehenik eta behin, programa bakoitzaren sarrera txiki bat agertuko da, bien arteko konparaketa batekin bukatzeko.

### 6.1.1. Veeam Backup

*Veeam Backup and Replication* segurtasun kopiak burutzen dituen software komertziala da. Aplikazio hau nahiko berria da, baina honen agerpenak izugarriko aldaketak sortu zituen segurtasun kopiak burutzen dituzten enpresen artean. Izan ere, RTO eta RPO denborak gutxi iraungo dutela bermatzen du. Ikusienez, denbora horiek oso garrantzitsuak dira enpresa batean, segurtasun kopiak berreskuratu behar direnean. Bere azpiegitura bezero/zerbitzari egituran dago oinarrituta. 6.1. taulan 4.1 atalean aipatutako ezaugarriak betetzen diren ziurtatuko dira eta zergatik.

Betebeharrak	Azalpena
Segurtasun kopia eta berreskuratze-koherentzia ziurtatzea.	Bai.
Zerbitzuaren eta negozioaren jarraipena bermatzea.	Bai, segurtasun kopien berreskurapena lortzeko gai delako. Oso indartsuak atal honetan RPO eta RTO denborak direla eta.
Informazioaren segurtasuna bermatzea.	AES 256-bit end-to-end zifratze algoritmoaren erabilera.
Negozioaren beste aplikazioarekin bateragarritasuna ziurtatzea.	Bai, gaur egun aukera gehien eskaintzen dituen softwarea da.
Memoria ziurtatzea.	Bai, datuak gorde ditzakeelako memoria fisikoan edota memoria birtualean.
Automatizazioaren eta informazioaren atxikipena ziurtatzea.	Bai, segurtasun kopiak eta berreskurapenak automatizatu daitezkeelako.
Txostenak sortzeko aukera eta erabilera egokia ziurtatzea.	Bai, interfaze grafiko intuitiboa duelako. Ingurunearen egoerari buruzko txostenak sortzeko aukera dago eta baita bezeroak bere txosten pertsonalak egiteko aukera.

6.1. taula. Veeam Backup ezaugarriak.

## 6.1.2. Arcserve UDP

Arcserve UDP sistema informatikoen datuak babesteko erabiltzen den programa da. Software honek, terminaletik urruneko fitxategi gunera soluzio integratua eskaintzen du. Programa ingurune fisiko eta birtualentzako arkitektura bateragarri batean oinarritzen da. *Backup*, dedupliakzioa eta *high availability* bezalako teknologien konbinaketa egiten da, denak batean bilduz. Honi esker organizazioek erraztasunak dituzte IT inguruneetatik eskalatzeko eta RTO eta RPO parametroen helburuak betetzeko, hurreneko kokalekuetan nahiz lainoan. *Backup* politika tradizionalak ordezkutzen dira, atazaz osatutako planen ordeiz. 6.2. taulan 4.1. atalean aipatutako ezaugarriak betetzen diren ziurtatuko dira eta zergatik.

Betebeharrak	Azalpena
Segurtasun kopia eta berreskuratze-koherentzia ziurtatzea.	Bai.
Zerbitzuaren eta negozioaren jarraipena bermatzea.	Bai, segurtasun kopien berreskurapena lortzeko gai delako.
Informazioaren segurtasuna bermatzea.	AES-256, AES-128, AES-192 algoritmoaren erabilera.
Negozioaren beste aplikazioarekin bateragarritasuna ziurtatzea.	Bai.
Memoria ziurtatzea.	Bai, datuak gorde ditzakeelako memoria fisikoan edota memoria birtualean.
Automatizazioaren eta informazioaren atxikipena ziurtatzea.	Bai, segurtasun kopiak eta berreskurapenak automatizatu daitezkeelako.
Txostenak sortzeko aukera eta erabilera egokia ziurtatzea	Bai, interfaze grafiko intuitiboa duelako. Ingurunearen egoerari buruzko txostenak sortzeko aukera dago eta baita bezeroak bere txosten pertsonalak egiteko aukera.

6.2. taula. Arcserve UDP ezaugarriak.

### 6.1.3. Konparaketa

#### Erabilera

Hasteko, *Arcserve UDP* programak, web interfazean oinarritutako kotsola bat du *Unified Management Console* (UMC) deritzona. Kotsola horren bitartez, administratzaileak, programaren funtzio guztien kontrola du. UMC-a erabiltzeko erraza, sinplea eta intuitiboa da, operazio edo funtzio bakoitzeko asistente baten laguntza erabiltzeko aukera izanik. Funtzio tipikoen artean hauek aurkitzen ditugu: Txostenak sortzeko aukera datu estatistikoekin, segurtasun kopia eta berreskuratze politikak ezartzeko aukera, segurtasun kopia programatzeko aukera etab. Argi dago, administratzaile baten lana kotsola baten bitartez askoz errazagoa dela, aipatu den bezala, kontrol guztia interfaze berdin batean dagoelako, beraz funtzio guztiak izateaz aparte, zerbitzari eta bezero guztiak kontrolatzen dira. *Veeam Backup* programak ere, kotsola baten bitartez kontrolatzen du *Backup* sistema guztia baina kasu horretan, mi metodo daude kotsola atzitzeko. Batetik, zerbitzarian instalatuta dagoen aplikaziotik eta bestetik web interfaze batetik.

Datuen ikusgarritasuna funtsezkoa da segurtasun kopia egiterako garaian. Bi programek editatu daitezkeen hainbat panel eskaintzen dituzte adibidez, segurtasun kopien egoera kontsultatzeko. Datuen estatistikak lortzerako orduan, *Veeam Backup* programak aukera gehiago eskaintzen ditu nahiz eta, bestean baino pauso gehiago jarraitu behar izan. Datuak era argiago eta zehatz batean azaltzen dira. Gainera, datu hauek beste aplikazio batera esportatzeko aukera eskaintzen du, besteak aldiz ez. Laburbilduz, bi programek erabilgarritasun eta eskalabilitate handia dute.

Hau guztia esanda, erabilera bi programetan egokia dela esango nuke eta oso antzekoa ere, nahiz eta *Veeam Backup*-en interfazea nire gusturako argiago eta erosoago den. Aipatuko nukeen desberdintasun nabariena kotsola atzitzeko modua da. Lehenengoaren kasuan, web bidez atzitu daiteke soilik, bigarrena aldiz, lokalki programaren bitartez eta web bidez.

#### Kostua

Kostuari dagokionez, *Arcserve UDP* programa *Veeam Backup* baino merkeagoa da.

Lehenengoari dagokionez, 6 lizentzia mota ezberdin aurkitzen dira: *Free*, *Workstation*, *Standard*, *Advanced*, *Premium* eta *Appliance*. Bakoitza aurrekoaren ezaugarri eta funtzioak hobetuz. Ondoren, aukera ezberdinen arabera eros daitezke lizentziak:

- *Socket* kopuruaren arabera.
  - Zerbitzari fisiko bat eta nahi diren zerbitzari birtualak zerbitzari berdinean babesteko aukera dago.
- Tamainaren arabera (TB).

- TB kopuruen arabera muga hori betetzen duten sistema guztiak babestu daitezke.
- Instantziaren arabera.
  - OS instantzia bat babesteko aukera dago zerbitzari fisiko edo birtual batean.

Proiektu honetan, "9 socket-en premium" lizentziarekin burutu da proiektua.

*Veeam*-en kasuan, lau lizentzia mota ezberdin aurkitzen dira: *Community*, *Standard*, *Enterprise* eta *Enterprise plus*. Bestean bezalaxe, aukera bakoitza aurrekoaren ezaugarri eta funtzioak hobetzen ditu. *Enterprise* lizentzia erosi beharko litzateke *Arcserve UDPren premium* lizentziaren funtzioak berdintzeko. Mota horretako lizentzia batek urtero 696 € balio ditu.

## Funtzioak

Orokorrean biek eskaintzen dituzte honako funtzioak eta modu eraginkorrean :

- Argazkien Backup-a, high availability, zintan edo lainoan.
- Deduplikazio global birtuala edo fisikoa.
- Erabiltzailearentzako interfazea, funtzio guztien kontrola bertan izanik.

*Arcserve UDP* programak puntu hauetan hobetzen du *Veeam Backup*-en zerbitzua:

- Deduplikazio eraginkorragoa eskaintzen du.
- UNC path-ak babestu ditzake, *Veeam* ek ordea UNC partekatuak.
- Unifikazioa. Dena batuta programa batean eskaintzen du, instalazio, interfaze eta lizentzia bakar batekin. *Veeam Backup* programari aldiz, zenbait modulu gehitu dakioke, funtzioak hobetuz. Adibidez *Veeam One* moduluari esker, monitorizazio atazak programa daitezke, automatizazio atazak programatu, etab.

Orokorrean ez daude diferentzia oso nabarmenak, beraz edozein software egokia izango litzateke *Backup* azpiegitura bat sortzeko.





# 7



## Ondorioak

## 7.1 Proiektuaren ondorioak

---

Azken kapitulu honetan proiektuan zehar atera diren ondorioak komentatuko dira.

Proiektuaren ikuspuntu orokor bat hartuta, esan daiteke proiektu honetako helburu nagusiak bete direla, nahiz eta proiektuan zehar zenbait arazo izan. Helburu nagusia, LYO egoitzan segurtasun kopiak garatzen dituen azpiegituraren konfigurazioa izan da. Horretarako, segurtasun kopiei buruzko zenbait kontzeptuen funtzionamendua ikasi da, hala nola, deduplikazioa, kopia motak, biltegiatze gailuen arteko desberdintasunak, RTO eta RPO parametroen garrantzia, etab. Kontzeptu hauek guztiak konbinatzen ikasi da, horrela planifikazio eraginkor bat lortuz. Horretaz aparte, enpresako eraginkortasuna handitzeko eta haiei laguntzeko *script* bat garatu da haiek egiten dituzten zenbait funtzio automatizatzeko.

Proiektuan zehar izandako arazoei aurre egiteko zailtasunak egon dira. Izan ere, enpresa batean eskatutakoa berehala eskaintzea prozesu motela da. Kasu honetan zenbait arazo egon dira programaren lizentziakin nik konpondu ezin nituenak. Beraz, planifikatutako egunean egiteko zeuden zenbait ekintza ezin izan dira garatu. Zenbait kasutan ere softwarearen zerbitzu teknikoarekin harremanetan jarri da erroreei konponbidea bilatzeko.

Horri aurre egiteko, aurretik planifikatutako arrisku plana kontsultatu da. Hori dela eta, beste ekintza batzuk paraleloki burutu dira. Gainera, aipatu beharra dago kontu handiarekin ibili behar dela beste zerbitzari batzuetara konektatzean, eta zenbait aldaketa egitean, izan ere, beste enpresa baten erremintak konfiguratzen ari baitzara. Normalean, zenbait aldaketa kritikoren aurrean, baimenak eskatu behar dira hauek burutzeko.

Laburbilduz, lortutakoarekin gustura geratu naiz, batez ere enpresa bateri eskaintzen zaion proiektua denez, lan munduan egiten den proiektu bat delako eta aurrerago horrelako lanak egitea tokatu ahal zaidalako. Planifikatutako guztia nahiko ondo bete da, ekintzak eta baita ere hauen egutegia. Esan beharra dago, gaur egun, proiektua martxan dagoela enpresan.

## 7.2 Ikasitakoa

---

Etorkizunera begira proiektuan zehar garatutako esperientzia positiboa izan da, izan ere proiektu honi esker jaso diren bi ezagutza nagusi azpimarratu nahi dira. Batetik proiektuan zehar, bereziki produktua garatzerakoan, ikasitako oinarri teoriko zein praktikoak. Bestetik, eta hau ondorio pertsonal bezala nabarmendu nahi da, proiektu bat zerotik garatzen hastearen zailtasuna bezero baten helburuak asebetetze arren. Bi ezagutza nagusi hauetaz aparte, orokorrean ikasitako kontzeptuak ondorengoak dira:

- Segurtasun kopiak burutzen dituen azpiegitura bat sortzen hasi aurretik erronka zaila eta oinarrizkoa dela jakin behar da enpresa batek bere zerbitzua ematen jarraitzeko. Beste modu batera esanda, zerbitzu hau ahula bada, enpresak datuak galtzeko arriskua izango du eta hondamendi baten aurrean, desagertzeko aukera.

- Hasieratik, enpresa, administratzailea bezain inplikaturik egon behar da proiektuan, izan ere, badaude zenbait kontzeptu enpresaren ardura direla horiek definitzea, RTO eta RPO denborak esaterako.
- Oso garrantzitsua da segurtasun kopiak gordeko diren kokalekuaren tamaina aurretik estimatzea eta planifikatzea, baita ere kokalekuari aplikatuko zaizkion erredukzio teknikak ere. Horrela prozesua exekutatzekoan, errore eta arazoak ekidinez.
- Arazo edo errore baten aurrean nola jokatu eta nola bilatu konponbidea.
- Planifikatutako planak exekutatu aurretik, birpasatzea eta egiaztatzea, produkzioan jarri baino lehen.
- *Script*-ak Windowsen programatzen ikastea.



## A Eranskina – *ARCserve UDP* Konfigurazioa

---

Eranskin honetan, *Arcserve UDP* programaren oinarrizko funtzioak nola burutu diren azalduko dira.

### Kontsolaren konexioa

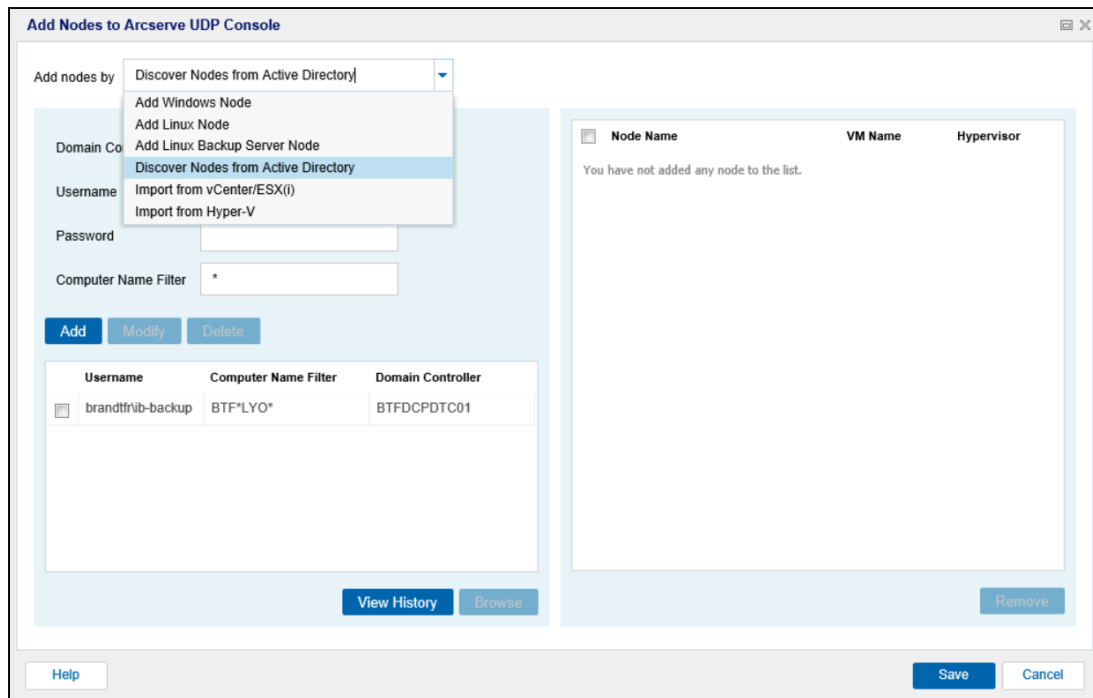
1. PMPko kontuaren kredentzialak sartu.
2. Konektatu BTFBKPLYO01 (Kontsola) zerbitzarira.
3. Internet erabiliz konektatu kontsolaren interfaze grafikora.
4. Kredentzialak sartu, programara konektatu ahal izateko.

### Nodoen gehikuntza

Funtzio hau burutzeko, bi era daude:

- **Era manuala**
  - Nodoa gehitu.
    1. “Resources”
    2. “All Nodes”
    3. “Add Nodes”
    4. Erabili nahi den metodoa aukeratu sistema eragilearen arabera. “Add Windows/Linux node”
    5. Zerbitzariaren IP helbidea edo izena sartu
- **Era automatikoa**
  - Nodoen detekzio metodoa konfiguratu. Honi esker egoitza baten nodo kopurua antzeman daiteke AD (*Active directory*) bitartez. Kasu honetan egunero 23:59tan konprobaketa hau egiten da.
    1. “Settings”
    2. “Node Discovery configuration”
  - Nodoa gehitu

1. "Resources"
2. "All Nodes"
3. "Add Nodes"
4. Erabili nahi den metodoa aukeratu. "Discover Nodes from Active Directory"



A.1. irudia. Nodoa gehitu.

## Agentearen instalazioa nodoetan

Kontsolarekin komunikatzeko nodo guztiek agentearekin harremanetan egon behar dute. Hori dela eta, agentearen instalazioa kontsula bitartez programatzen da.

1. Nodoa aukeratu
2. "Actions"
3. "Install/Upgrade Agent"

## Kokalekua espezifikatu

Kokalekua, segurtasun kopiak gordeko diren zerbitzaria izango da. Jarraian kokalekua ezartzeko aukerak azalduko dira, proiektuan aukeratutako kokalekuaren azalpen zehatzagoa burutuz.

- **Recovery Point Server (RPS):** Hainbat nodoen datuak gorde daitezke eta ondoren datu hauek berreskuratu nahi direnean. Instalatu baino lehen zenbait aurre baldintza bete

behar ditu. Lehenik, sistema eragilea Windows Server 2008 R2 baino berriagoa izatea, agentea zerbitzarian instalatuta egotea eta azkenik, kotsola instalatuta izatea. Metodo hau erabili da.

1. "Resources"
2. "Destinations"
3. "Recovery Point servers"
4. "Add a Recovery Point Server" (A.2. irudia)
5. BTFBKPLYO01-n sortu da RPSa.

**Add a Recovery Point Server**

A Recovery Point Server offloads resource-intensive tasks from the Arcserve UDP Agent and enables features like global deduplication and catalog generation.

Node Name/IP Address: BTFBKPLYO01

Username: BRANDTFRlib-backup

Password: .....

Description:

Installation Location: E:\

Port: 8014

Protocol:  HTTP  HTTPS

**!** HTTPS is recommended for secure communication. If the node is an RPS, use of HTTPS will encrypt data over the wire.

Change Tracking Driver:  Install Agent Change Tracking Driver

The driver is needed if you want to perform backup of this system. However it is not needed if this system

A.2. irudia. RPS-a gehitu.

- **Arcserve Backup Servers:** Datuak zintan gorde nahi ezkeru, aukera hau erabili beharko da.
- **Karpeta konpartituak**
- **Lainoa:** Erabiltzaileak lainoan duen kontu bat erabiliz, segurtasun kopiak bertan gordetzeko aukera.

## Datu biltegia sortu

Datu biltegia, segurtasun kopiak gordetzeko erabiliko den lekua izango da. Kasu honetan aurreko pausoen, BTFBKPLYO01 zerbitzarian sortutako RPS-ean sortu da datu biltegia, A.3. irudian agertzen den bezala.

**Create a Data Store**

View general rules or estimate storage capacity requirements for deduplication in the [Requirements Planning Quick Reference](#).

Settings to enable or disable deduplication, compression and encryption cannot be changed after the data store creation process.

Recovery Point Server	BTFBKPLYO01		
Data Store Name	<input type="text" value="Backup"/>		
Data Store Folder	<input type="text" value="E:\Data Store"/>	<input type="button" value="Browse"/>	
Concurrent Active Nodes Limit to	<input type="text" value="4"/>		
<input checked="" type="checkbox"/> Enable Deduplication			
Deduplication Block Size	<input type="text" value="16 KB"/>	<input type="checkbox"/> Deduplication	<input type="checkbox"/> Tape Backup
Hash Memory Allocation	<input type="text" value="1024"/>	MB (Maximum: 32733 MB; Minimum: 1024 MB)	

A.3. irudia. Datu biltegia sortu.

1. Datu biltegia non kokatuko den ezarri.
2. Datu biltegian ea deduplikazio teknika aplikatu nahi den edo ez.
3. Deduplikazio blokeen tamaina ezarri. Geroz eta blokearen tamaina handiagoa izan, geroz eta deduplikazio teknikak eraginkortasun txikiagoa izango du, baina berreskuratzeke ahalmen eta azkartasuna lortuko du.
4. Konprimaketa teknika aplikatu edo ez, diskoaren tamaina gehiago murriztuz.

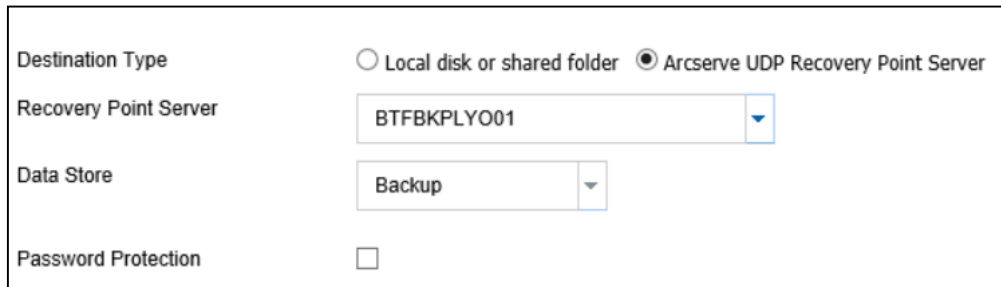
## Plan bat sortu

Nodo bat babesteko beharrezkoa da plan bat sortzea. Plan bat segurtasun kopiak kudeatzeko hainbat ataza dira. Ondorengo pausoak jarraitu behar dira plan bat sortzeko:

1. "Name and Type"
  - a. Planari izena ipini.
  - b. Plan mota aukeratu (*Backup: Agent-Based Windows* edo *Backup: Agent-Based Linux*). Sistema eragilearen arabera plana ezberdina izango da. Fitxategi zehatz baten segurtasun kopia egin nahi bada, *Backup: Files on UNC or NFS Path* mota aukeratu beharko da. Ondoren nahi diren fitxategien kokalekuaren *path*-a sartuz.
2. "Source"
  - a. Plan hori aplikatu nahi zaien nodo edo nodoak aukeratu behar dira.
  - b. Segurtasun kopia zeri egin nahi zaion aukeratu. Bolumen guztiei edo bolumen zehatz bati.



3. "Destination" (A.4. irudia)



Destination Type  Local disk or shared folder  Arcserve UDP Recovery Point Server

Recovery Point Server

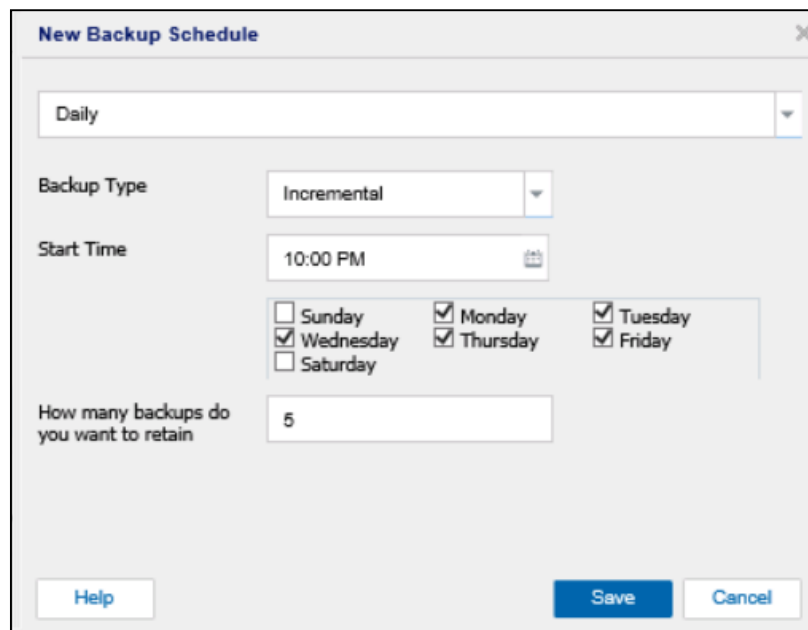
Data Store

Password Protection

A.4. irudia. "Destination" konfigurazioa.

- a. Segurtasun kopiak non gorde nahi diren espezifikatu.
- b. Segurtasun kopien segurtasuna bermatzeko hauei pasahitza ezartzeko aukera.

4. "Schedule" (A.5. irudia)



New Backup Schedule

Daily

Backup Type

Start Time

Sunday  Monday  Tuesday  
 Wednesday  Thursday  Friday  
 Saturday

How many backups do you want to retain

Help Save Cancel

A.5. irudia. "Schedule" konfigurazioa.

- a. Segurtasun kopia mota ezarri (Inkrementala, Osoa edo Verify).
- b. Periodoa eta ordua ezarri (Egunero, astero, hilero).
- c. Kopien erretentzio kopurua ezarri, hau da, gorde nahi diren kopien kopurua ezabatu hasi aurretik.

5. "Advanced"

- a. segurtasun kopientzako *Snapshot* mota ezarri.

- b. Zenbait aplikazioen (*SQL server* edo *Exchange Server*) erregistroak ezabatzeo aukera.
- c. *Script*-ak exekutatzeko aukera segurtasun kopia burutu baina lehen eta ondoren. Hala nahi bada, *script*-a non kokatzen den zehaztu beharko da.
- d. Korreo elektronikoan abisuak ezartzeko aukera. Egoera desberdinetan abisua bidaltzeko aukera (Diskoaren tamainaren %80 betea badago, segurtasun kopia ez bada burutu, etab.).

## Segurtasun kopia manuala programatu

Edozein momentuan exekutatu daiteke segurtasun kopia bat. Horretarako aukeratu nodoa eta ondorengo pausoak jarraitu :

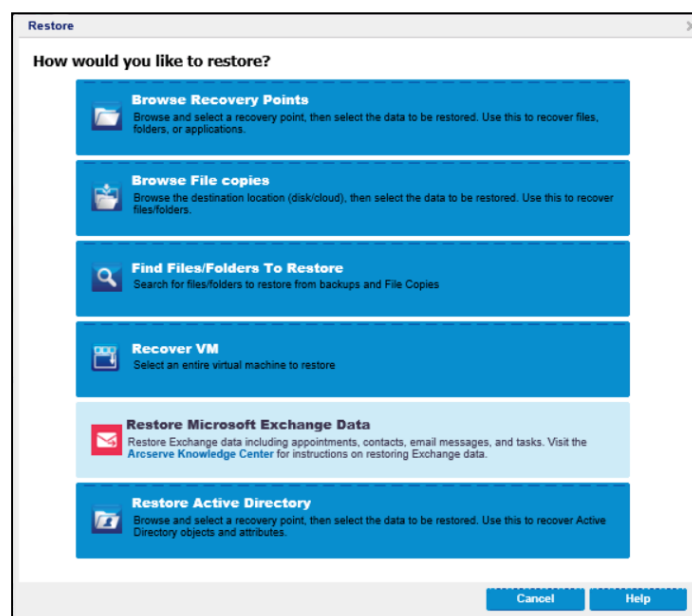
1. "Actions"
2. "Backup now"

## Segurtasun kopien berreskurapena

Berreskuratu nahi diren nodo edo nodoak aukeratu eta ondorengo sakatu beharko da :

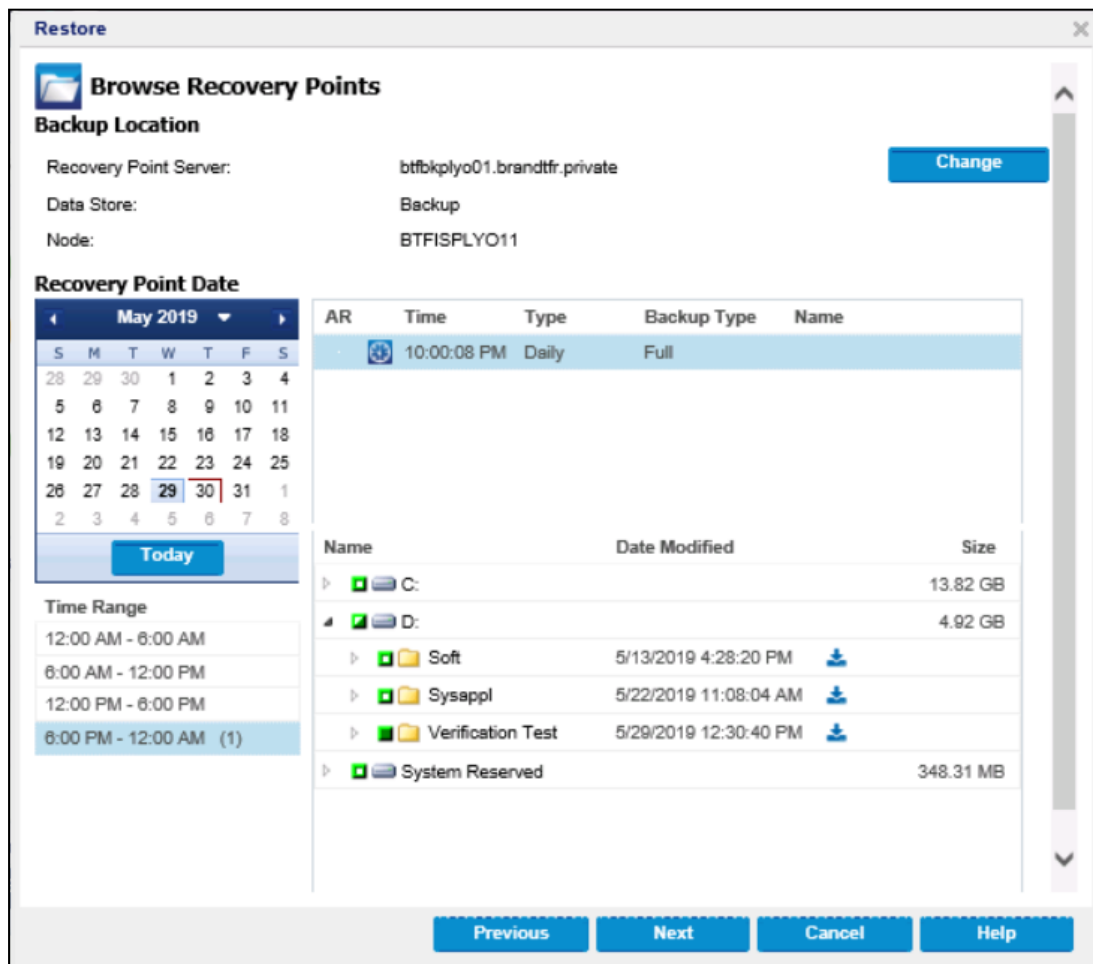
1. "Actions"
2. "Restore"

Aukeratutako nodoaren agentearen interfazera konektatuko da eta informazioa berreskuratzeko ze metodo aplikatu nahi den aukeratu beharko da, A.6. irudian agertzen diren aukeretatik.



A.6. irudia. "Backup Recovery" motak.

Lehenengo aukera sakatzen bada, oraingoz sortuta dauden segurtasun kopiak agertuko dira eta erabiltzaileak erabaki beharko du zein puntutik berreskuratu nahi duen informazioa. A.7. Irudian ikusten den bezala, C:/, D:/ eta sistemarentzat erreserbatuta dauden datuen unitateak berreskuratzeko aukera dago. Unitate bakoitzaren barruan dagoen datu karpeta edo artxiboa soila ere berreskuratu daiteke.



A.7. irudia. Artxiboen aukeraketa.

Azkenik, datuak non berreskuratu nahi diren aukeratu beharko da. Bi aukera daude, batetik, kokaleku originalean berrezartzea edo bestetik, erabiltzaileak zehazten duen kokaleku batean. Datuak kopiatzean arazoren bat balego ere, hauekin zer egin zehaztu behar da.

- Existitzen diren artxiboak ordezkatu : Fitxategiak berrezarriko diren kokalekuan, hauek existitzen badira, ordezkatu egingo dira.
- Existitzen diren artxibo aktiboak ordezkatu: Fitxategiak berrezarriko diren kokalekuan, hauek existitzen badira eta erabiltzen ari badira, sistema berrabiaraztean ordezkatu egingo dira.

- Artxiboen izenak aldatu: Artxiboaren izena existitzen bada, beste berri bat sortuko du.
- Existitzen diren artxiboak baztertu: Fitxategiak berrezarriko diren kokalekuan, artxibo berdin bat aurkitzen bada ez da kopiatuko, originala utziz.

Prozesua konfiguratu ondoren, automatikoki artxiboak berrezartzen hasiko da.

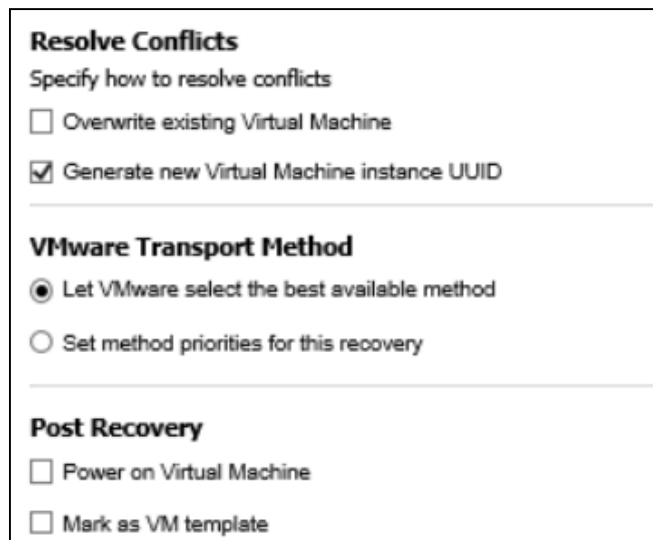
“Recover VM” aukera sakatzen bada, zerbitzari birtual baten berrezartzea burutuko da. Lehenik eta behin, ze egunetik aurrera berrezarri nahi den aukeratu behar da eta ondoren non sortu nahi den makina birtual berria. Bi aukera existitzen dira:

- Kokaleku originalean berrezartzea.
- Beste kokaleku batean berrezartzea.

Bigarren aukera jarraitzea erabaki bada, *Vmware ESXi* zerbitzariaren ezaugarriak sartu beharko dira, A.8. irudian agertzen den bezala.

A.8. irudia. Makina birtual bat berrezartzeko aukerak.

LYO egoitzan sortu den makina birtuala denez, egoitza horretako ESXi zerbitzaria (42.0.100.101) ezarri da, baimenak dituen erabiltzaile batekin. Ondoren, makina birtualaren izena ezarri behar da eta baita ze inguruneetan gordeko den. Kasu honetan, proba bat denez “QA&DEV” ingurunean sartu da. Erro zerbitzari honen ze datu biltegi gorde nahi den makina birtuala ere ezarri behar da.



The image shows a dialog box with three sections: 'Resolve Conflicts', 'VMware Transport Method', and 'Post Recovery'. Each section contains radio or checkbox options.

Section	Option	Selected
Resolve Conflicts	Overwrite existing Virtual Machine	<input type="checkbox"/>
	Generate new Virtual Machine instance UUID	<input checked="" type="checkbox"/>
VMware Transport Method	Let VMware select the best available method	<input checked="" type="radio"/>
	Set method priorities for this recovery	<input type="radio"/>
Post Recovery	Power on Virtual Machine	<input type="checkbox"/>
	Mark as VM template	<input type="checkbox"/>

A.9. irudia. Makina birtual bat berrezartzeko aukera aurreratuak.

Azkenik, ea makina berria sortzen den edo zaharraren gainean ordezkatzeko erabaki behar da eta piztu gabe utziko da, A.9. irudian ikusten den bezala. Hala egiten da, produkzioan dagoen zerbitzari bat delako, beraz, erabiltzaile batek zerbitzari originala nahas dezake berriarekin, izena aldatzen ez den kasuan adibidez.



## B Eranskina – Emaitzak

Atal honetan proiektuan zehar neurtu diren probak eta haien emaitzak agertuko dira.

BTFISPLYO01 zerbitzariaren segurtasun kopia mota desberdinak biltegitratze gailu desberdinetan

- Zintan:

Mota	Denbora	Babestutako datuen tamaina	Erabilitako Tamaina	Redukzioa (D+C)
Osoa	0:20:14	16.9 GB	16.9 GB	EZ
Inkrementala	0:04:02	2.3 GB	2.3 GB	EZ

B.1. taula. Zintan kopiatu diren BTFISPLYO01 zerbitzariaren emaitzak.

- Diskoan:

Mota	Denbora	Babestutako datuen tamaina	Erabilitako Tamaina	Redukzioa (D+C)
Osoa (1) <sup>2</sup>	0:54:49	16.9 GB	8.85 GB	%52.36
Osoa (hiler) <sup>3</sup>	0:08:51	17.2 GB	0.3 GB	%98.27
Inkrementala	0:04:28	1.29 GB	0.31 GB	%76.53

B.2. taula. Diskoan kopiatu diren BTFISPLYO01 zerbitzariaren emaitzak.

<sup>2</sup> Zerbitzari horri aplikatu zaion lehenengo segurtasun kopia osoa.

<sup>3</sup> Zerbitzariari hiler aplikatzen zaion segurtasun kopia osoa.

BTFISPLYO05 proba zerbitzarien segurtasun kopia mota desberdinak diskoan

Mota	Denbora	Babestutako datuen tamaina	Erabilitako Tamaina	Redukzioa (D+C)	Data
Osoa (1)	2:29:35	108.13 GB	85.11 GB	%21.29	23-5-19 22:00
Inkrementala	0:02:31	1.19 GB	0.4 GB	%65.99	24-5-19 22:00
<i>Verify</i>	0:07:47	108.13 GB	0..03 GB	%99.96	24-5-19 22:00
Inkrementala	0:03:15	2.1 GB	0.8 GB	%59.90	27-5-19 22:00
<i>Verify</i>	0:09:06	108.8 GB	0.04 GB	%99.96	27-5-19 22:00

B.3. taula. BTFISPLYO05 proba zerbitzariaren emaitzak.

LYO egoitzako zerbitzarien emaitzak diskoan

Zerbitzaria	Mota	Denbora	Babestutako datuen tamaina	Erabilitako Tamaina	Redukzioa (D+C)
BTFISPLYO11	Osoa (1)	0:55:00	16.31 GB	10.44 GB	%36
BTFISPLYO11	Osoa (hilero)	0:04:07	16.32 GB	0.04 GB	%99.75
BTFISPLYO11	Inkrementala*	0:01:06	0.37 GB	0.04 GB	%88.16
BTFDCPLYO01	Osoa (1)	0:50:02	18.6 GB	8.31 GB	%55.34
BTFDCPLYO01	Osoa (hilero)	0:07:15	18.62 GB	0.38 GB	%98
BTFDCPLYO01	Inkrementala*	0:04:37	2.04 GB	0.47 GB	%78.86
PARTAGES (BTFFSPLYO01)	Osoa (1)	24:48:36	328.79 GB	328.01 GB	%29.56

B.4. taula. LYO egoitzako beste zerbitzarien emaitzak.

\* Lortutako emaitza guztien batz bestekoak dira



Beste egoitza bateko zerbitzarien emaitzak

Zerbitzaria	Mota	Denbora	Babestutako datuen tamaina	Erabilitako Tamaina	Redukzioa (D+C)
BTFISDDTC01	Osoa	5:40:09	41.14 GB	30 GB	%28
BTFISDDTC01	Inkrementala	0:19:30	1.43 GB	676 MB	%54

B.5. taula. Beste egoitza bateko zerbitzarien emaitzak.

BTFISPLYO11 zerbitzarian karpeta baten berreskuratzea

Mota	Denbora	Errekuperatutako datuen tamaina
RP (Osoa)	0:00:02	1.6 GB
RP (Inkrementala)	0:00:03	1.6 GB

B.6. taula. BTFISPLYO11 zerbitzariaren berreskuratze denborak.

BTFISPLYO11 makina birtualaren berreskuratzea

Mota	Denbora	Errekuperatutako datuen tamaina
RP (Agenterik gabe)	1:06:36	41.12 GB

B.7. taula. BTFISPLYO11 makina birtualaren berreskuratzea.



## C Eranskina – Bilera Aktak

---

Proiektuaren garapenaren zehar egindako bilera guztien nondik norakoak bildu dira eranskin honetan.

Bilera guztiak leku berean eta parte-hartzaile berdinekin egin dira:

**Lekua:** Informatika Fakultateko 214 bulegoa (Zuzendariaren bulegoa).

**Partaideak:** Jose Antonio Pascual eta Ion Molla.

### B.1 Konstituzio Bilera

Data:

2019/04/15, 16:00

Helburuak:

Proiektuaren nondik norakoak komentatu.

Bileran hitz egindakoa eta hartutako erabakiak:

Proiektuaren nondik norakoak eta helburuen azalpena komentatu diot tutoreari. Tutorea ados dagoela helarazi dit.

Egin beharrekoak:

Konstituzio bilera denez, lehenengo kontaktua izateko bilera bat da, beraz, eginbehar bakarrak gradu amaierako lanaren sarrera aurreratzea eta hurrengo bileraren data zehaztea dira.

### B.2 Lehenengo Bilera

Data:

2019/05/08, 16:00

Helburuak:

Dokumentuari hasiera ematea. Tutoreak eskainitako txantilo batetik.

Bileran hitz egindakoa eta hartutako erabakiak:

Dokumentuaren sarrera eta planifikazio atalak eginda eraman ditut. Segurtasun kopien aurrekarien eta moten atala ere eginda ekarri dudanez, begirada bat eman diogu. Tutoreak

komentatu dit argazkietan akatsa dudala. Hori konpontzeko, lortutako web orriari erreferentzia egin behar diot. Hartutako erabaki garrantzitsuak:

- Astean behin elkartzea erabaki dugu, horrela jarraipen zehatzago bat lortuz.
- Kapitulu oso bat burutzean, tutoreari bidaliko zaio hark zuzentzeko eta hobekuntzak aipatzeko.

Egin beharrekoak:

*ARCServe UDP* programaren erabilera ikasten joatea, horrekin batera dokumentua aurrera eramatea.

### **B.3 Bigarren Bilera**

Data:

2019/05/15, 16:00

Helburuak:

Dokumentuaren egoera aztertu eta akatsak zuzentzea. Enpresan egindakoa komentatzea.

Bileran hitz egindakoa eta hartutako erabakiak:

Dokumentazioari dagokionez zenbait akats identifikatu dira:

- Argazki batzuk ezabatu eta besteei iturria ipini.
- Argazki edo taula batek kapitulu baten amaiera ez izatea.
- Sarrera atala gehiago landu eta sakondu.

Egin beharrekoak:

Dokumentazioa zuzendu eta *Arcserve UDP* programarekin hasi.

### **B.4 Hirugarren Bilera**

Data:

2019/05/22, 16:00

Helburuak:

Astean aurreratua eta egindakoa (programarekin lehenengo segurtasun kopiak programatzea) komentatzea.

Bileran hitz egindakoa eta hartutako erabakiak:

Dokumentuari dagokionez:

- Inpertsonalaren erabilera bultzatzea.
- Hainbat sigla eta akronimo daudenez glosario bat egitea erabaki da.

Garapenari dagokionez:

- Lehenengo fasea ezin izan da bukatu, segurtasun kopiak ez direlako burutu, lizentzia arazoak direla eta. Beraz, konpondu arte ezin da probatu.

Egin beharrekoak:

Dokumentua eguneratu, proba fasea amaitu eta emaitza horiek analizatu.

## **B.5 Laugarren Bilera**

Data:

2019/06/05, 16:00

Helburuak:

Bidalitako dokumentuaren hirugarren bertsioa komentatzea, zuzentzea eta egiteko geratzen dena argitzea.

Bileran hitz egindakoa eta hartutako erabakiak:

Dokumentazioari dagokionez:

- Zenbait akats ortografiko zuzendu.

Garapenari dagokionez:

- Segurtasun kopiak burutzean izandako arazoak komentatu dira eta haiei emango zaien soluzioa.

Egin beharrekoak

Hurrengo bilerarako proiektua ia bukatu izatea da helburu nagusia. Horretarako *script-a* garatzen bukatuko da, programen arteko konparaketa egiten saiatuko da eta azkenik, hobekuntza proposamenak atala garatzen hasiko da.

## B.6 Bosgarren Bilera

Data:

2019/06/19, 16:00

Helburuak:

Bidalitako dokumentuaren laugarren bertsioa komentatzea, zuzentzea eta egiteko geratzen dena argitzea.

Bileran hitz egindakoa eta hartutako erabakiak:

- Dokumentuaren egoerari buruz hitz egin da.
- Egin behar den posterraren espezifikazioak argitu dira.
- Planifikazio txiki bat egin da noiz dokumentua eta posterraren lehen bertsioa noiz egingo den argituz.

Egin beharrekoak

Hurrengo bilerarako dokumentua bukatuta egon behar du. Posterraren lehenengo bertsio bat entregatu beharko da tutoreari.

## B.7 Seigarren Bilera

Data:

2019/07/03, 16:00

Helburuak:

Dokumentuaren eta posterraren erroreak zuzentzea eta komentatzea.

Bileran hitz egindakoa eta hartutako erabakiak:

- Posterrean laburpen txiki bat sartzea komeni da.

Egin beharrekoak

Posterraren bertsio finala burutu eta dokumentuaren erroreak zuzendu.

## Bibliografía

---

- [1] YURIN, M (). *The history of backup*. <http://www.backuphistory.com/>
- [2] SASSONE, S (2015). *La evolución de los soportes de backup*. <https://www.somoseset.com/2015/04/01/evolucion-soportes-backup/>
- [3] INFORMÁTICA PARA TU NEGOCIO. *Ventajas y desventajas de los diferentes tipos de backup*. <https://www.informaticaparatunegocio.com/blog/ventajas-desventajas-los-diferentes-tipos-backup/>
- [4] (Oct 12, 2018). *Backup types*. <https://www.backup4all.com/backup-types-kb.html>
- [5] FELLOWS, R (2008). *Copia de seguridad completa, incremental o diferencial: cómo elegir el tipo adecuado*. <https://searchdatacenter.techtarget.com/es/cronica/Copia-de-seguridad-completa-incremental-o-diferencial-como-elegir-el-tipo-adecuado>
- [6] WIKIPEDIA. *Unidad de cinta*. [https://es.wikipedia.org/wiki/Unidad\\_de\\_cinta](https://es.wikipedia.org/wiki/Unidad_de_cinta)
- [7] ARCSERVE. *Arcserve UDP*. <https://www.arcserve.com/es/data-protection-solutions/arcserve-udp/>
- [8] ARCSERVE. *Guía de soluciones de Arcserve Unified Data Protection*.
- [9] ARCSERVE. *Rps datastore – deduplication and best practices*. <https://www.arcserve.com/es/data-protection-resources/rps-datastore-deduplication-and-best-practices/>
- [10] GILART IGLESIAS, I (15 diciembre, 2016). *Claves para escoger el enfoque de deduplicación en el backup según el sistema a respaldar*. <http://www.whitebearsolutions.com/claves-para-escoger-el-enfoque-de-deduplicacion-en-el-backup-segun-el-sistema-a-respaldar/>
- [11] RIVERA, P (25 Octubre, 2017). *Diferencias entre RPO y RTO*. <https://www.2ksystems.com/blog/14-blog-sistemas-servidores/199-diferencia-entre-rpo-y-rto>
- [12] Ultrium LTO (1999). *What is LTO technology?*. <https://www.lto.org/technology/what-is-lto-technology/>
- [13] BERTRAND, C (2017). *Informe técnico de producto*. [http://www.arcserve.com/wp-content/uploads/sites/19/2017/05/Arcserve-udp-technical-product-white-paper\\_8000\\_SPA.pdf](http://www.arcserve.com/wp-content/uploads/sites/19/2017/05/Arcserve-udp-technical-product-white-paper_8000_SPA.pdf)