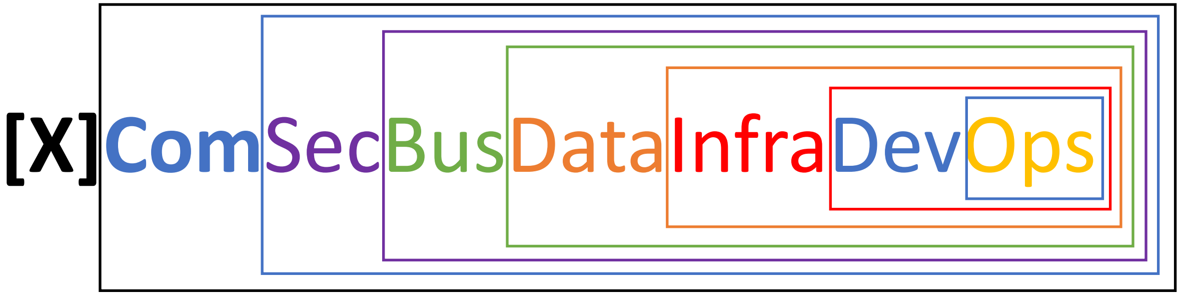
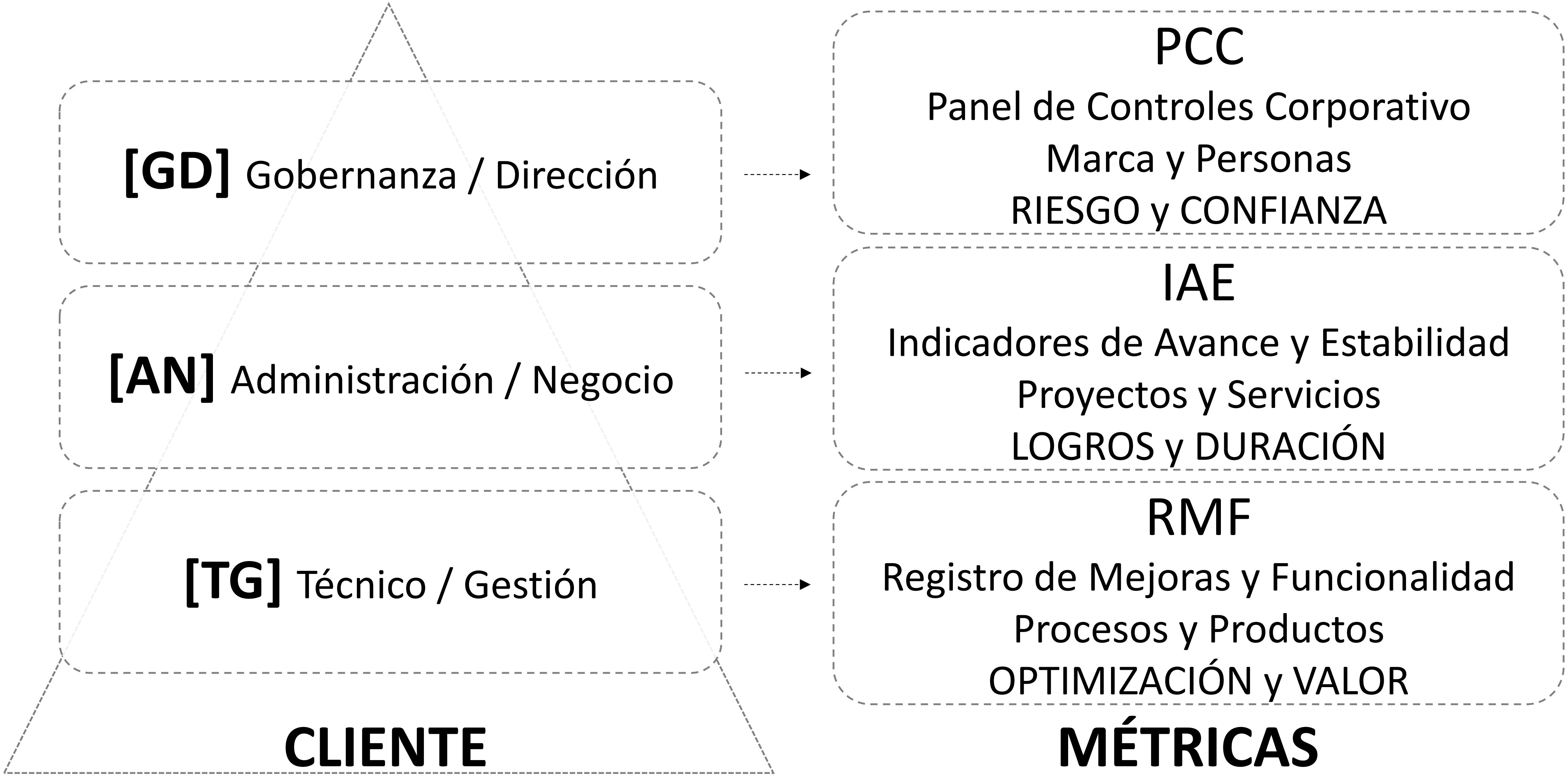


[X]ComSecBusDataInfraDevOps



[GD] Gobernanza / Dirección

[AN] Administración / Negocio

[TG] Técnico / Gestión

CLIENTE

PCC

Panel de Controles Corporativo

Marca y Personas

RIESGO y CONFIANZA

IAE

Indicadores de Avance y Estabilidad

Proyectos y Servicios

LOGROS y DURACIÓN

RMF

Registro de Mejoras y Funcionalidad

Procesos y Productos

OPTIMIZACIÓN y VALOR

MÉTRICAS

ÁREAS

1 Compliance

2 Cyber Security

3 Business

4 Data

5 Infrastructure

6 Development

7 Operations

FUNCIONES

1.1 Regulación y normativa: ENS, LOPD-GDD, RGPD, ISO, SGSI, NIST, PCI-DSS, SCRUM, GRC, OWASP, AGILE, SDLC, RFC, IEEEComputerSociety
1.2 Riesgos 1.3 Auditoría
2.1 Proveedores/Fabricantes
2.2 Desarrollo de negocio
2.3 Preventa
3.1 Ciclo del dato
3.2 Análisis de datos
4.1 Prevención 4.2 Detección
4.3 Respuesta 4.4 Resiliencia
5.1 On-prem 5.2 Cloud
6.1 Frontend 6.2 Backend
6.3 Fullstack 6.4 INGSW
7.1 Ticketing y alertas

TECNOLOGÍAS Y HERRAMIENTAS

1.1.1 Adobe, MSOffice
1.2.1 PILAR 1.3.1 Archer
2.1.1 CheckPoint, CyberArk, FireEye, Fortinet, Google, Linux, Microsoft, Palo Alto Networks, RSA, Symantec
3.2.1 BD, ML, MATLAB, SPSS St. IBM, EXCEL, MySQL, SQLite
4.1.1 Nessus, NMAP, Kali Linux, DSA
4.2.1 IDS, EDR, SIEM 4.3.1 IPS, FW, WAF, GPMC 4.4.1 HA, CDN
5.1.1 Router, Switch, HSM, Diode, Proxy, VM, CMDB, AD, Windows, UNIX
5.2.1 Azure, O365 5.2.2 GCP
6.1.1 HTML5, CSS3, JQUERY, Javascript
6.2.1 SQL, Java, C, C#, Python, Dart/Flutter, PHP/Symfony, API, PowerShell, VS, Android, iOS
6.3.1 MVC 6.4.1 Git, DEV, QA, PROD
7.1.1 ServiceNow, logs

AREAS

1 Compliance

2 Cyber Security

3 Business

4 Data

5 Infrastructure

6 Development

7 Operations

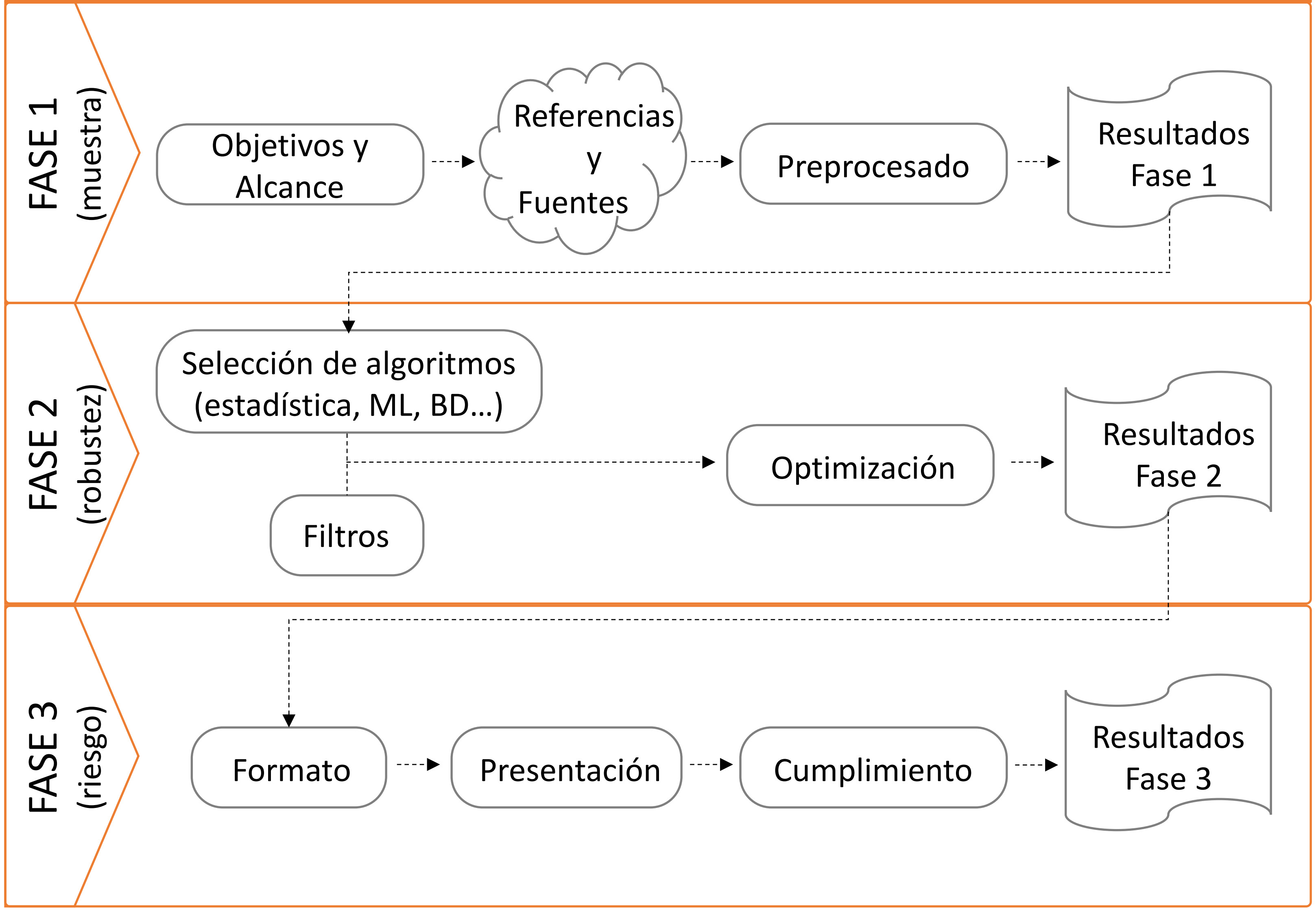
JOB FUNCTIONS

1.1 Policies and standards: ENS, LOPD-GDD, RGPD, ISO, SGSI, NIST, PCI-DSS, SCRUM, GRC, OWASP, AGILE, SDLC, RFC, IEEEComputerSociety
1.2 Risks **1.3** Assessments
2.1 Manufacturers
2.2 Business development
2.3 Presales
3.1 Data lifecycle
3.2 Data analysis
4.1 Prevention **4.2** Detection
4.3 Response **4.4** Resilience
5.1 On-prem **5.2** Cloud
6.1 Frontend **6.2** Backend
6.3 Fullstack **6.4** INGSW
7.1 Ticketing y alerts

TECNOLOGY TOOLS

1.1.1 Adobe, MSOffice
1.2.1 PILAR **1.3.1** Archer
2.1.1 CheckPoint, CyberArk, FireEye, Fortinet, Google, Linux, Microsoft, Palo Alto Networks, RSA, Symantec
3.2.1 BD, ML, MATLAB, SPSS St. IBM, EXCEL, MySQL, SQLite
4.1.1 Nessus, NMAP, Kali Linux, DSA
4.2.1 IDS, EDR, SIEM **4.3.1** IPS, FW, WAF, GPMC **4.4.1** HA, CDN
5.1.1 Router, Switch, HSM, Diode, Proxy, VM, CMDB, AD, Windows, UNIX
5.2.1 Azure, O365 **5.2.2** GCP
6.1.1 HTML5, CSS3, JQUERY, Javascript
6.2.1 SQL, Java, C, C#, Python, Dart/Flutter, PHP/Symfony, API, PowerShell, VS, Android, iOS
6.3.1 MVC **6.4.1** Git, DEV, QA, PROD
7.1.1 ServiceNow, logs

Metodología Análisis de Datos



FASE 1 (muestra)

Objetivos y Alcance

Referencias y Fuentes

Preprocesado

Resultados Fase 1

FASE 2 (robustez)

Selección de algoritmos (estadística, ML, BD…)

Filtros

Optimización

Resultados Fase 2

FASE 3 (riesgo)

Formato

Presentación

Cumplimiento

Resultados Fase 3

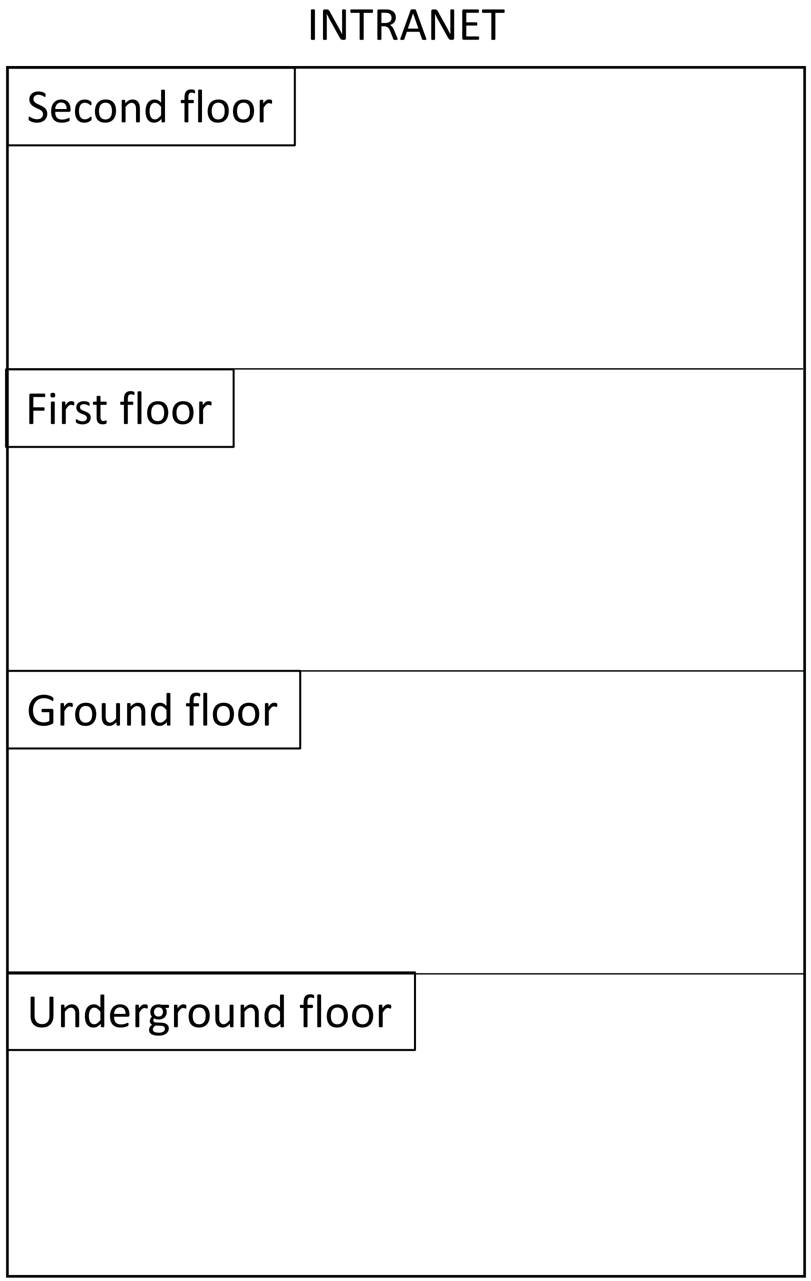
The basis on IT Infrastructure is CONNECTIVITY

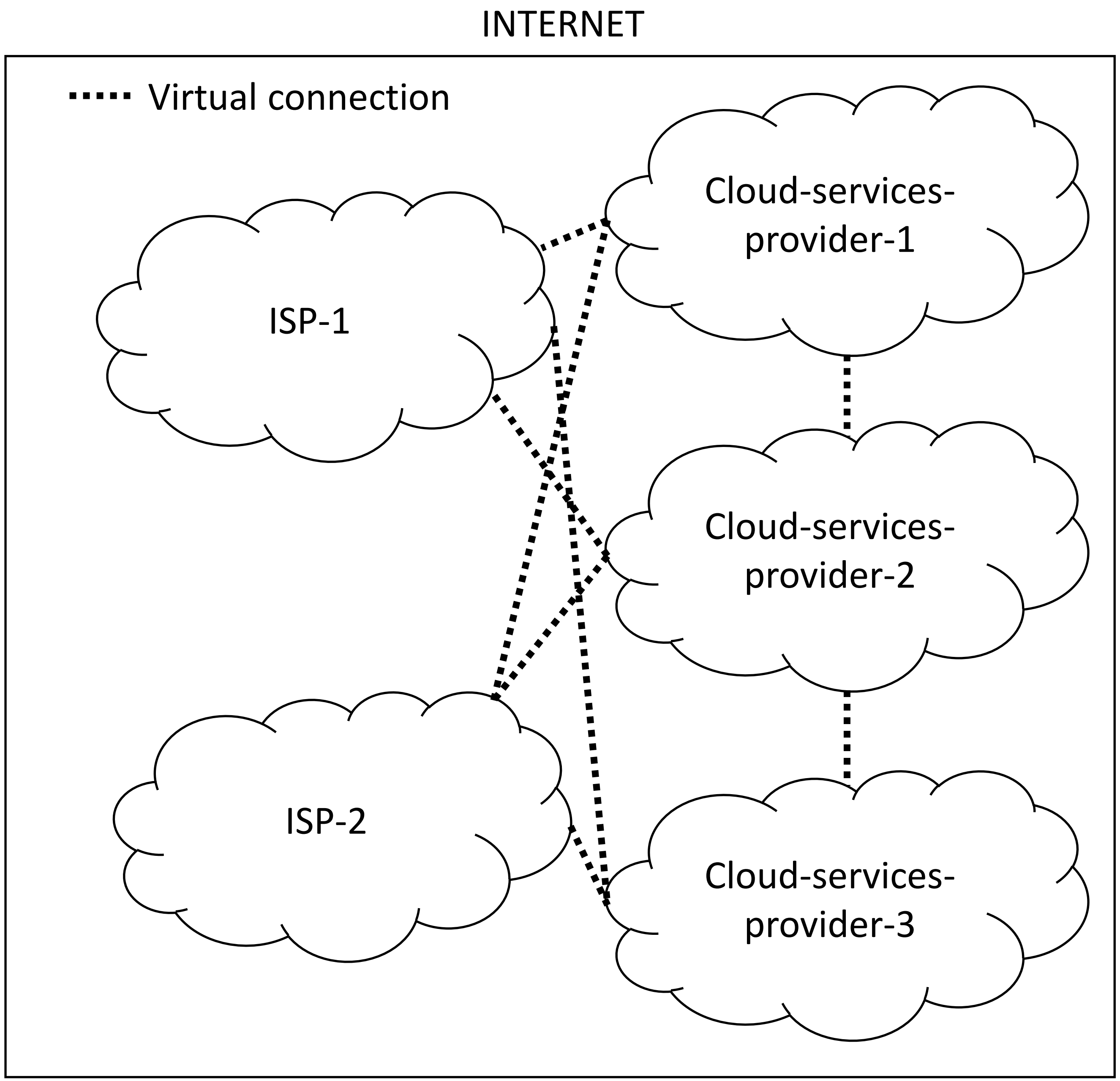
The minimum recommended network components are:
2 ISP providers with their corresponding routers
2 Firewalls
2 main high-performance switches
2 WiFi controllers
And depending on the number of floors and the floor extention, the rest of switches for cable connectivity and Access Points to Wireless connectivity

It is mentioned two of them because there are the principal and the contingency ones for any kind of connectivity disruption

What kind of questions I will think about?

Is it correctly cable across the office – labeling each one and for proper maintenance wheather changes are needed – with their RJ-45 connectors?
Do you have two ISP providers (the principal and the contingency one) hired?
Are network components – firewalls, routers, switches – configured by following best practices?
Are this configurations currently saved it as backups daily and/or when changed it?
Do you know what is the current bandwith – bps – in different parts of your office? Are you monitoring this?
Are you doing connectivity exercises and documenting everything encountered by the following scenarios?
Scenario-1: Unplug the principal ISP, thus contingency ISP must give connectivity (how many minutes long until this


INTRANET
Second floor
First floor
Ground floor
Underground floor


INTERNET
Virtual connection
Cloud-services-provider-1
ISP-1
Cloud-services-provider-2
ISP-2
Cloud-services-provider-3