Toutes les données sont stockée en interne dans des datacenters, accès gérer par badge et mdp

Rétention de 10 ans sur l’archivage.

Journée de formation lors de la première journée sur sécuritl etc

Politique sécuritl : reverentiel des normes et standarts basés sur ISO 27001

Audit : Audit technique : scan chaque mois et personnes viennent audité chaque année d’un point de vue technique et organisationnel

Annuaire directory : toutes les authorisasion se font par l’AD (domaine applicatif)

Les prods sont repliquer sinsco sur 2 date center et sauvergarder

Dataloss, contrôle des accès internets

Accèes physique badge et code

Tracabilité : AD , savoir qui a fait quoi

Virus : verif mail, sur tous nos postes, control des flux http et https

Réseaux : isolé par des firewall

Logs : grose bd on on centralise tous nos logs , rechercher dessus, ces logs sont vérifié par une entreprise ( machine learning)

Cryptage/ chiffrement : https, sauvegardes sur cassette externalisée sont chiffrées, accès application et serveurs sont chiffrés (SSL, HTTPS)