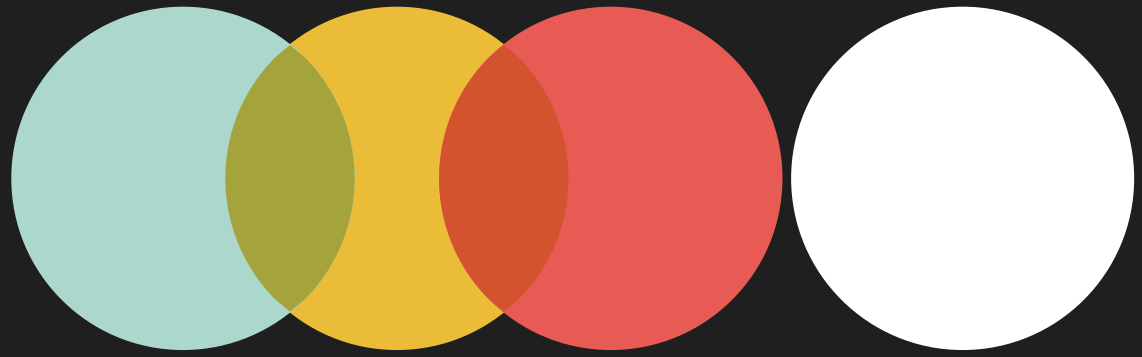
SIGMA-RH



Conférence HR Tech

Sécurité informatique et des données sensibles et confidentielles : Comment mieux gérer les données de vos employés dans votre système RH.

Présentée par Patrice Poirier

14 avril 2022

SIGMA-RH en quelques mots

SIGMA-RH accompagne les moyennes et grandes entreprises dans l'optimisation de leurs processus de gestion des ressources humaines en offrant un logiciel **SIRH** fiable, flexible, évolutif et personnalisable, favorisant le partage des informations et la réalisation d'économies de temps et d'argent.

SIGMA-RH

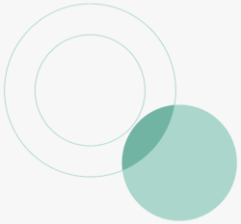
SIGMA-RH en quelques chiffres

30 ans

d’expérience en développement logiciel

20 pays

dans lesquels les solutions sont déployées



3 millions

de dossiers employés gérés

15 modules

pour une couverture globale

Contexte

Lois et réglementations

SIGMA-RH

Historique des lois

1982

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels au Québec.

1993

Loi sur la protection des renseignements personnels dans le secteur privé au Québec.

27 avril 2016

RGPD encadre le traitement des données personnelles sur le territoire de l'UE.

2016

Première version de SecNumCloud en France.

12 juin 2020

Québec dépose son projet de loi 64.

Nov. 2020

Ottawa introduit le projet de loi C-11 sur la mise en œuvre de la Charte du numérique.

25 mars 2022

Nouveau cadre transatlantique de protection de la confidentialité des données de l'UE.

2022

Loi 25_Phase 1

2023

Loi 25_Phase 2

2024

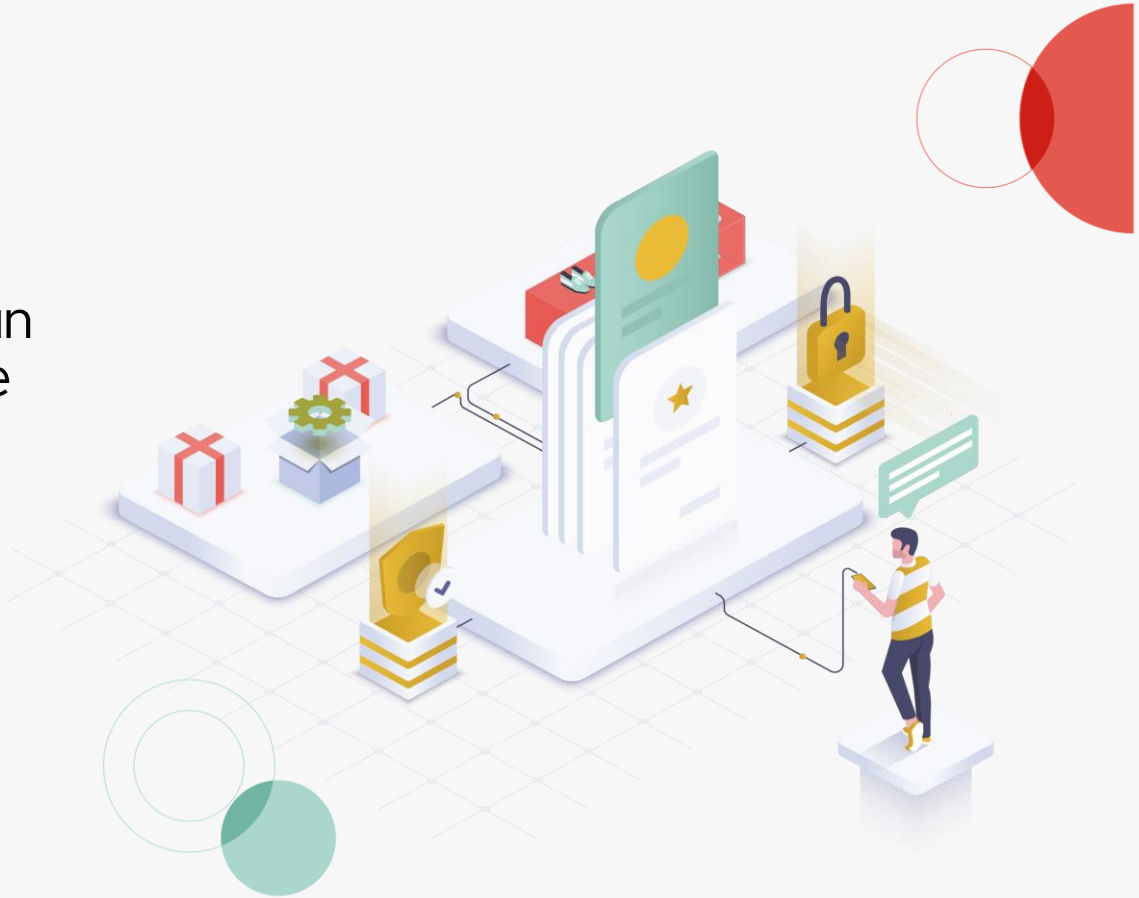
Loi 25_Phase 3

SIGMA RH

Qu'est-ce qu'une donnée à caractère personnel?

Tout renseignement personnel ayant identifié ou permettant d'identifier une personne physique.

Elles ne s’appliquent pas aux renseignements personnels pouvant servir à l'identifier dans l'exercice de ses fonctions, tel qu'un nom, prénom, titre, courriel, et numéro de téléphone de son lieu de travail.



SIGMA RH

La Loi 25 résumée (anciennement Projet de loi n° 64)

Septembre 2022

- Nomination d'un **responsable** de la conformité des **processus** et **procédures** liés à la protection des renseignements personnels.
- Obligation d'aviser la Commission d'accès à l'information (CAI) de tout incident de confidentialité impliquant un renseignement personnel présentant un risque sérieux de préjudice.
- Obligation de former un **comité** sur l'accès à l'information et la protection des renseignements personnels. Ces mesures doivent être **publiées sur le site web** de l'entreprise.
- Obligation de divulguer toute banque de caractéristiques ou de mesures biométriques à la Commission au moins 60 jours avant sa mise en service

SIGMA RH

La Loi 25 résumée (anciennement Projet de loi n° 64)

Septembre 2023

- L’obligation de **publier les règles** encadrant sa gouvernance à l’égard des renseignements personnels.
- Publication d'une **politique de confidentialité.**
- Mise en place d’un processus de traitement des plaintes.
- Déploiement de pratiques et politiques de conservation de la donnée répondant entre autres à "comment et quand sera-t-elle détruite?".
- Évaluation des facteurs relatifs à la vie privée lors de toute refonte, acquisition ou développement d’un système d’information ou prestation de service.
- **Formation de sensibilisation**

SIGMA RH

La Loi 25 résumée (anciennement Projet de loi n° 64)

Septembre 2023

- Toute entreprise se doit de **détruire** tout renseignement personnel lorsque les fins auxquelles il a été recueilli ou utilisé sont accomplies, sous réserve d'un délai de conservation prévu par une loi.
- Elle pourrait les **anonymiser** pour les utiliser, mais uniquement à des fins sérieuses et légitimes.
- Les organismes publics pourront faire de même, strictement à des fins d'intérêt public.

SIGMA RH

La Loi 25 résumée (anciennement Projet de loi n° 64)

Septembre 2023

Sanctions administratives imposées

- Amende maximale de 10M pour les entreprises ou 2% du chiffres d'affaires mondiale pour une multinationale.
- Poursuites pénales jusqu'à 10K pour une personne physique et 25M ou 4% du chiffre d'affaires pour une entreprise.
- TPE peut souvent être une personne physique.
- En cas de récidive les sanctions peuvent doubler.

SIGMA RH

L’importance de la sécurisation des données

SIGMA-RH

Menaces externes et internes

Attaques externes

Profil	Pirates informatiques
Origine	Malveillance
Volume de données mis à risque	Extrêmement élevé
Fréquences	Limitée (mais en augmentation rapide)

35.5 %

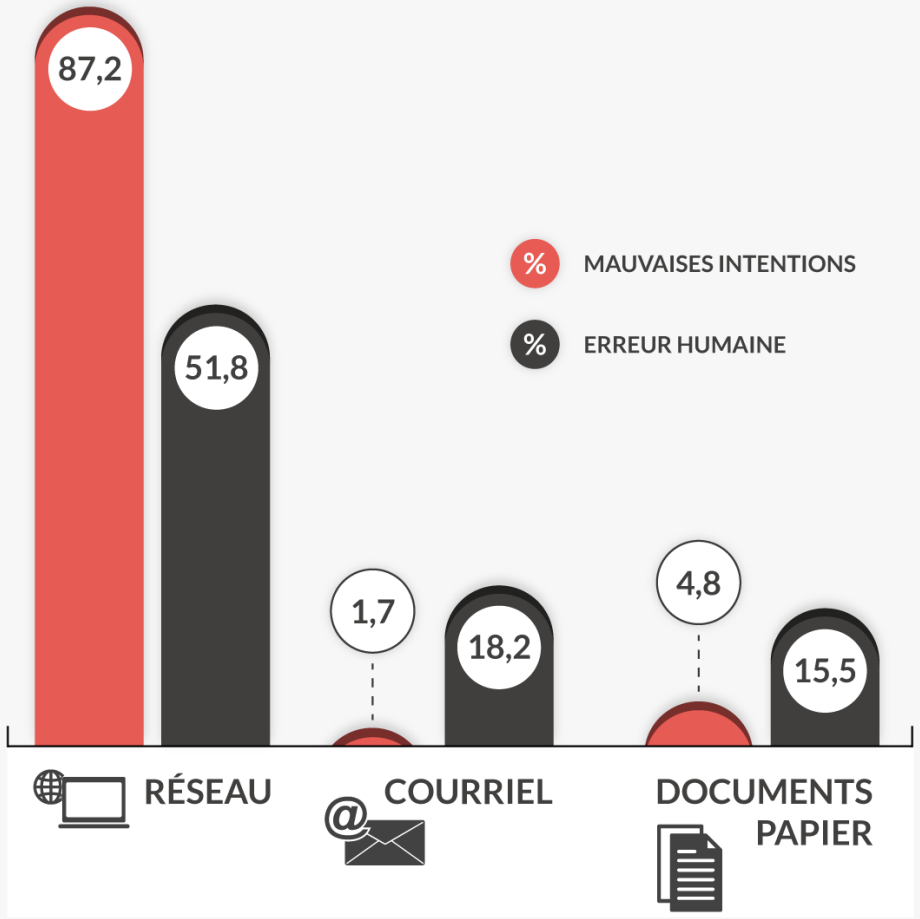
Fuites de l’interne

Profil	Tout employé
Origine	Inattention, négligence, parfois malveillance
Volume de données mis à risque	Faible
Fréquences	Extrêmement élevée

64,5 %

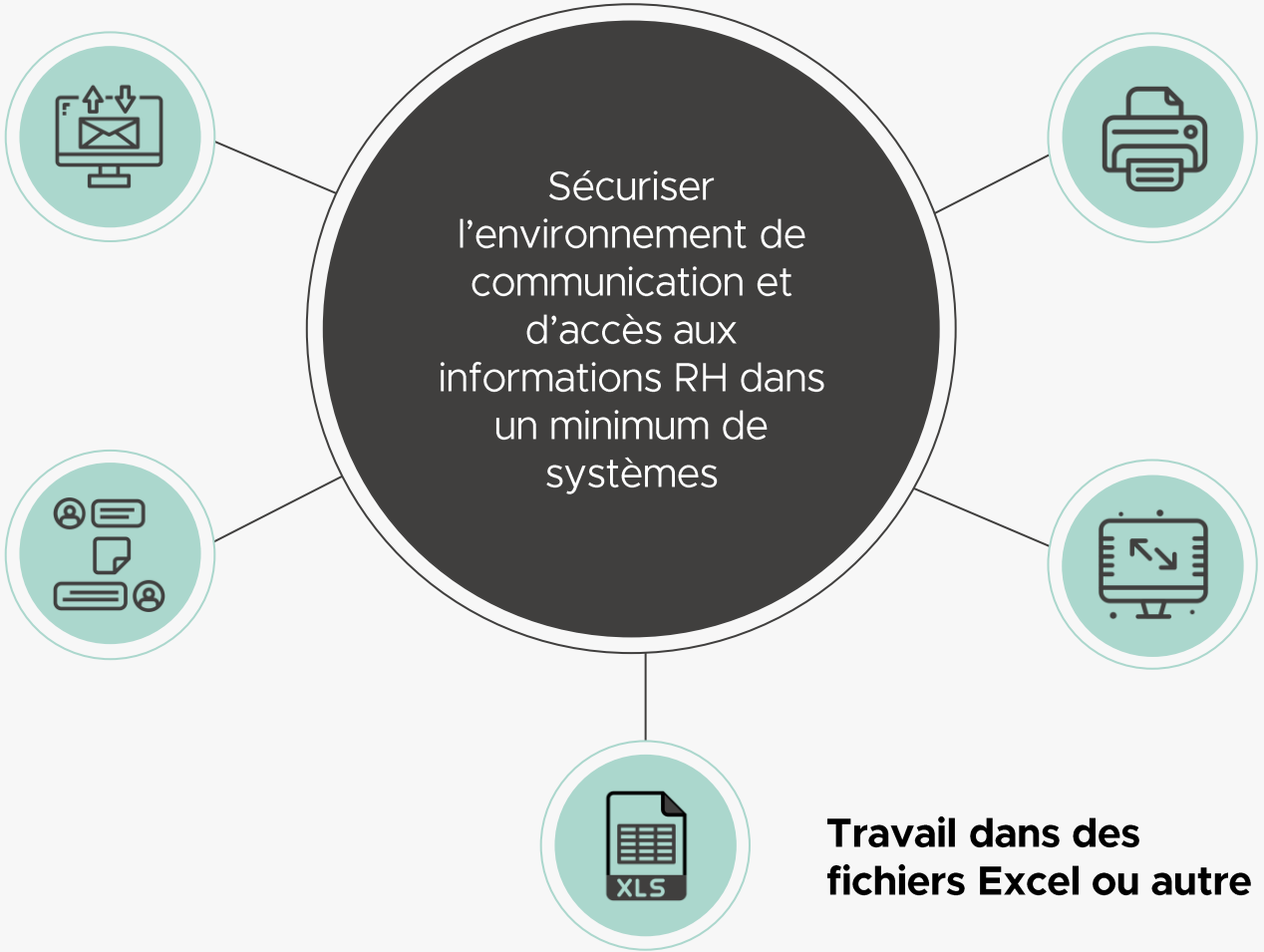
SIGMA RH

Statistiques clés



SIGMA-RH

Pratiques où les données sont à risque



Envoi de courriels

Impression de documents sur papier

Systèmes de gestion multiple

Partage d'écran

Travail dans des fichiers Excel ou autre

SIGMA RH

Comment sécuriser les données avec un SIRH

SIGMA-RH

La multiplication des systèmes ou la multiplication des risques

LÉGENDE

Systèmes

Logiciel de la gestion de temps
Gestion de la formation
Gestion des évaluations
Gestion des griefs
Logiciel de note de frais
Liste de rappel, dossiers administratifs
Bases de données internes
Paie
Recrutement, mesures disciplinaires, visites médicales, prêts d'équipements, contrats de travail (SharePoint, LMS, libre-service employé

Données

Informations personnelles
NAS
Salaire, bonus, déductions
Formations, certification
Absence
Temps travaillé

Menaces

Hameçonnage
Cyberattaque
Fraude
Fuite de données

SIGMA RH

Cas client - 800 employés

5 systèmes gérant des données RH :

- Paie
- Gestion des temps
- Talents (formation et entretiens annuels)
- Recrutement
- Portail employé agrégateur

23 fichiers Excel contenant des données personnelles :

- Listes d'employés par département
- Dossiers de relations de travail
- Dossiers d'accidents de travail
- Liste d'ancienneté (avec trop d'information)

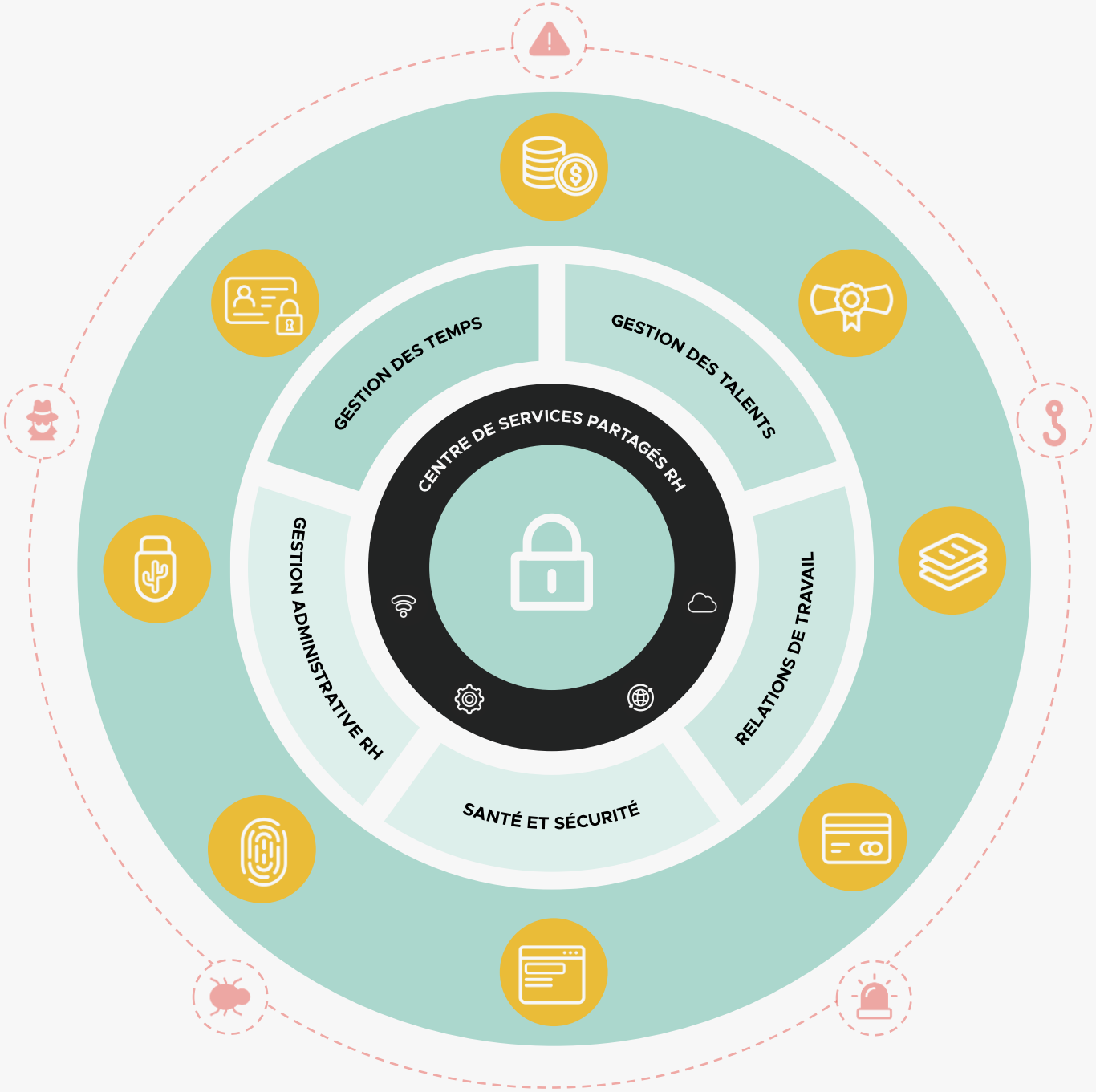
RÉSULTAT:

- 2 systèmes restants
- 26 portes fermées sur 28
- 2 fournisseurs sécures
- Niveau de risque faible

SIGMA RH

Centralisation des données RH

1. Centralisez
2. Sécurisez
3. Limitez les systèmes
4. Limitez les accès
5. Appliquez le principe du moindre privilège



SIGMA RH

Travaillez avec des entreprises certifiées

Quelques exemples de certifications à rechercher ou à exiger

ISO 27001

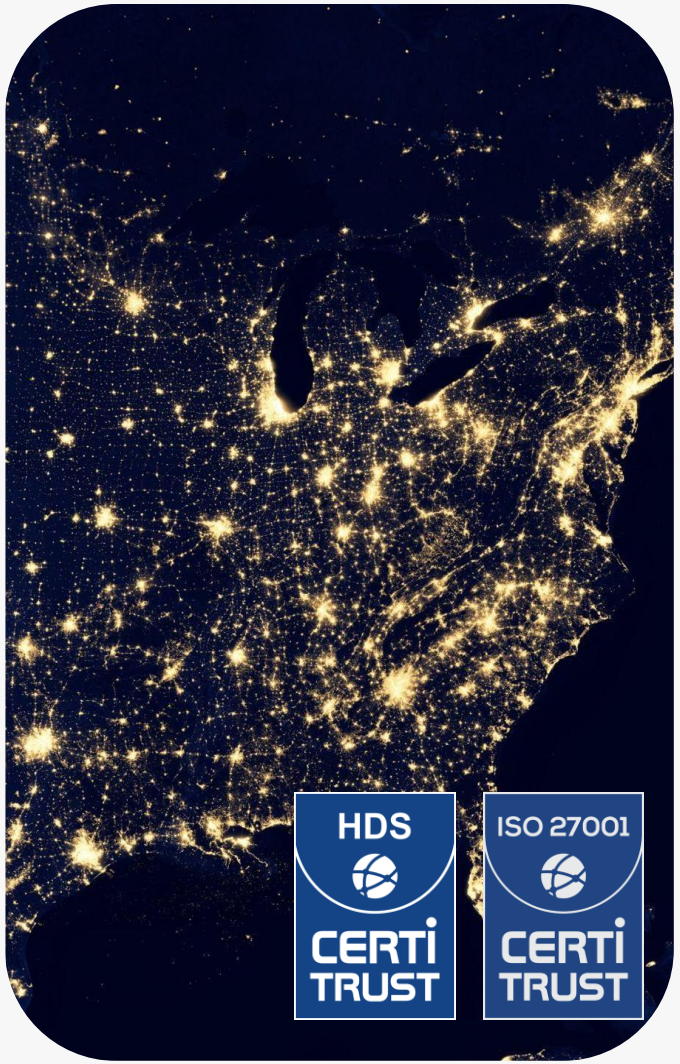
- Norme internationale
- Couvre la sécurité de l'information dans son ensemble
- Vision globale de la sécurité basée sur un audit adapté
- Audit effectué par des personnes certifiées pour ISO 27001

SOC 2 type 2

- Norme américaine
- Peut couvrir un processus ou un système uniquement
- Démontre la sécurité d'un système basé sur des questionnaires statiques
- Audit effectué par un expert comptable (CPA)

HDS (Hébergement de Données de Santé)

- Norme française
- Encadre les obligations des fournisseurs ayant accès à des données de santé



SIGMA-RH

Conclusion

- Mettez en place un plan de déploiement de mesures et procédures face à l'adoption de la nouvelle Loi 25 dès maintenant.
- Apportez soutien à l’organisation et aux employés sur ces changements de pratiques.
- Entourez-vous de partenaires technologiques avisés, possédant les certifications adéquates lors de la venue de la nouvelle législation.

SIGMA RH

Période de questions

SIGMA RH

SIGMA-RH

Merci de votre participation

Pour en savoir plus, visitez-nous au kiosque 101