WEB-CONFÉRENCE CLUSIF
30 JUIN 2020

MENACES INFORMATIQUES ET PRATIQUES DE SÉCURITÉ EN FRANCE

Collectivités territoriales

Actualités du Clusif

REFONTE DE NOS OUTILS COLLABORATIFS

FINALISATION DES TRAVAUX DE RENOVATION

MIPS 2020

Une restitution présentée par

Lionel MOURER le 25 juin 2020
MANIKA
Responsable de l'étude et de la partie Entreprises

Cyril BRAS le 30 juin 2020
GRENOBLE-ALPES MÉTROPOLE
Responsable de la partie Collectivités territoriales

Jérôme NOTIN le 7 juillet 2020
GIP ACYMA
Responsable de la partie Internautes

CLUSIF

Webconférence organisée grâce au soutien de nos sponsors

HS2 Hervé Schauer Sécurité

ilex International

proofpoint.

TERRANOVA SECURITY

RESTITUTION MIPS 2020 : PRÉSENTATION DE L'ÉTUDE

Lionel MOURER

ADMINISTRATEUR CLUSIF

PRÉSIDENT MANIKA

✓ Objectifs de l'enquête 2020

Établir un état des lieux des pratiques de sécurité et de la sinistralité de l'information en France

Déterminer les tendances générales en matière de sécurité de l'information

✓ Rapports

Par thème : publié après chaque présentation

Complet : le mercredi 8 juillet 2020

Disponibles sur le site du CLUSIF

✓ Démarche retenue

Questionnaire élaboré par un groupe de travail du CLUSIF

09 à 12-2019

Enquête confiée à un cabinet d'étude marketing spécialisé (GMV Conseil)

01 à mi-03-2020

Résultats analysés par un groupe d'experts membres ou non du Clusif

mi-03 à mi-06-2020

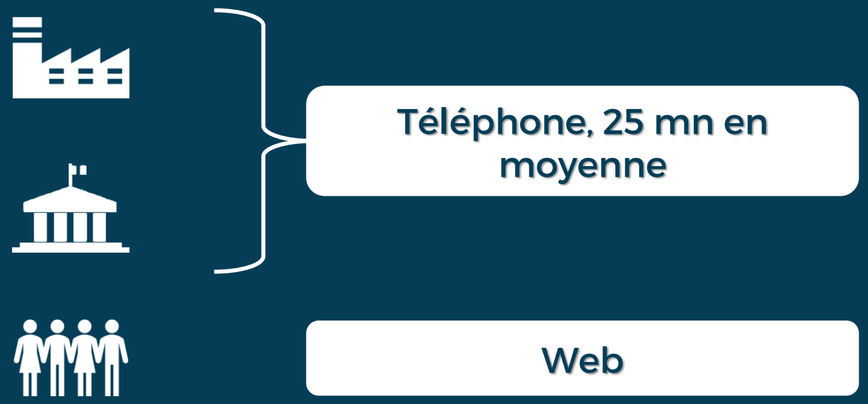
25-06, 30-06 et 07-07 : restitutions des résultats

08-07 : publication du rapport complet

MIPS : un guide pour tous les acteurs du domaine de la sécurité de l'information

- ✓ **Enquête réalisée en T1-2020 et portant sur les données 2019**
- ✓ **Réalisée sur 3 cibles différentes**
  - Les entreprises de plus de 100 salariés (350)
  - Les collectivités territoriales (202)
  - Les internautes (998)

- ✓ **Échantillon statistiquement représentatif**
  - Chiffres redressés selon l'INSEE



MIPS : une enquête de référence basée sur un échantillon large et représentatif

Entreprises et Collectivités territoriales : un questionnaire « exhaustif » basé sur les thèmes de l'ISO 27002

- ✓ Thème 5 : Politique de sécurité de l'information
- ✓ Thème 6 : Organisation de la sécurité de l'information
- ✓ Thème 7 : Sécurité des ressources humaines
- ✓ Thème 8 : Gestion des actifs
- ✓ Thème 9 : Contrôle d'accès
- ✓ Thème 10 : Cryptographie
- ✓ Thème 11 : Sécurité physique et environnementale
- ✓ Thème 12 : Sécurité liée à l'exploitation
- ✓ Thème 13 : Sécurité des communications
- ✓ Thème 14 : Acquisition, développement et maintenance des systèmes d'information
- ✓ Thème 15 : Relations avec les fournisseurs
- ✓ Thème 16 : Gestion des incidents liés à la sécurité de l'information
- ✓ Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- ✓ Thème 18 : Conformité

Internautes : un questionnaire en 4 volets

- ✓ Profil des internautes et inventaire informatique
- ✓ Perception et sensibilité aux menaces et aux risques
- ✓ Usages des internautes
- ✓ Moyens et comportements de sécurité

« Spéciale dédicace » !

MERCI !!!

- ✓ **Aux responsables de thèmes**
- ✓ **Aux expert(e)s qui ont contribué à l'élaboration du rapport**
- ✓ **Au président et au CA du Clusif qui nous font (toujours) confiance**
- ✓ **Aux permanentes du Clusif**

RESTITUTION MIPS 2020 : COLLECTIVITES TERRITORIALES

CYRIL BRAS

✓ Remerciements

Aux 202 collectivités ayant participé à l'étude

- 31 communes de plus de 30 000 habitants
- 34 communautés de communes de plus de 10,000 habitants
- 111 communautés d'agglomération, urbaines et métropoles
- 26 conseils territoriaux

Les 21 experts en cybersécurité ayant analysé les résultats

✓ Présentation

Méthode des quotas utilisée pour représenter au mieux la réalité des collectivités françaises.

16 % des collectivités sollicitées ont répondu

20 % des répondants étaient des RSSI

La SSI dans les collectivités

✓ Quels constats ?

Une dépendance à l'informatique toujours forte

Un budget dédié à la SSI

- Méconnu
- Non pérenne d'une année sur l'autre
- Variable d'ajustement ?
- Mais en progression ou constant pour la majorité

✓ Pourquoi ?

Transformation numérique en route

57% refuse de le communiquer

Mais qui permet d'en déduire si le sujet est traité à son juste niveau par rapport à la taille de la collectivité

OU

D'en déduire une cyberattaque ayant affecté la collectivité

La SSI dans les collectivités

✓ Politique de Sécurité de l'Information

Des progrès dans la formalisation de la PSI

Qui sont majoritairement maintenues à jour

Basée sur une ou plusieurs normes

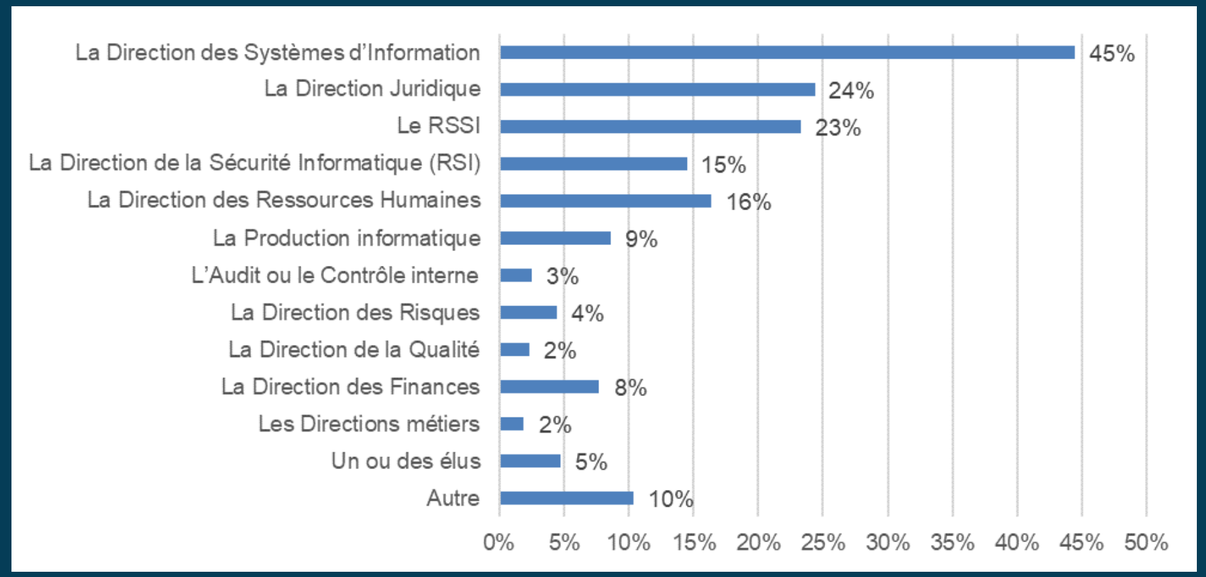
MAIS

Qui reste encore moyennement diffusée hors des DSI

Moyennement soutenues par les DGS

ALORS QUE

Les DGS sont impliqués dans l'élaboration pour 70 % des cas



Entités impliquées dans la PSI

La SSI dans les collectivités

✓ Le RSSI acteur de la SSI ?

Mieux en mieux identifié

Fonction dédiée dans 59 % des collectivités

MAIS

Difficile à dédier pour 1/3 des collectivités

Plutôt réservé aux plus grandes structures

La SSI n'est pas encore à portée de tous !

✓ Les difficultés du RSSI ?

Fonction partagée avec celles de :

- DSI 42 %
- Responsables informatiques 37 %
- Consultants externes 20 %

ENTRAINANT

- des difficultés de compréhension des enjeux par l'encadrement dirigeant
- des doutes sur les capacités à révéler les défaillances, les incidents

MAIS AUSSI

Un positionnement qui ne permet pas de libérer totalement la parole !

La SSI dans les collectivités

✓ Du point de vue humain ?

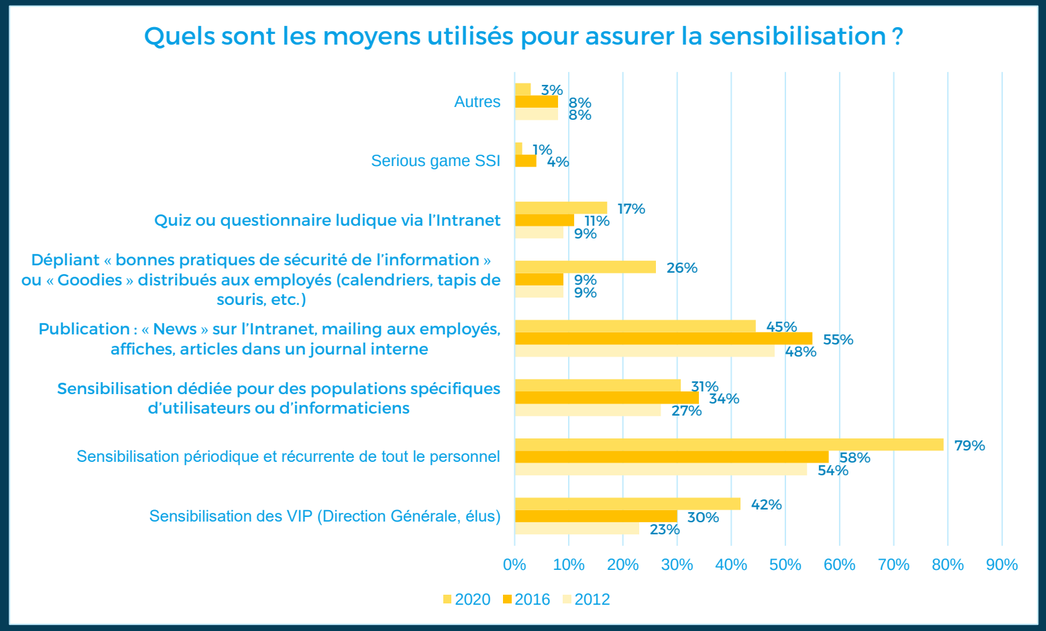
Des effectifs consacrés à la SSI souvent insuffisants

Une gestion des départs ou changement de poste trop rarement adressée

Une charte d'usage s'appliquant :

- Aux personnel 97 %
- Aux prestataires et fournisseurs 37 %
- Quid des élus ?

✓ Et la sensibilisation ?



La SSI dans les collectivités

✓ Quelle prise en compte des actifs ?

Un inventaire et une classification en progression X4 en 4 ans

MAIS

Mis en place par seulement 1/5 des collectivités

La classification se limite à sensible ou non sensible pour plus de 40 %

✓ Et au niveau des risques ?

Un inventaire réalisé

MAIS

sans analyse formelle

ALORS QUE

Des plans de réduction sont mis en place

Les risques seraient ils en fait traités de façon empirique ?

La SSI dans les collectivités

✓ Comment l'accès au SI est il contrôlé ?

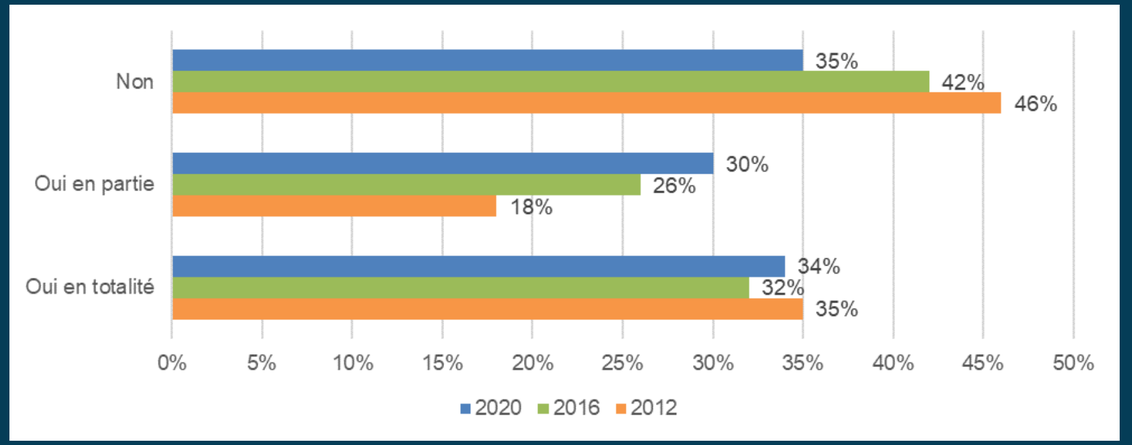
Homogénéisation des moyens de contrôle

Améliorations dans les procédures de gestion

Notamment pour les administrateurs

64 % ont défini des politiques de complexité et de renouvellement des mots de passe

Néanmoins il y a des disparités entre les différentes collectivités



Règles de constitution et de péremption des mots de passe

La SSI dans les collectivités

✓ Protection de l'information

Seulement 35% des collectivités utilisent le chiffrement de l'information pour :

- sécuriser des données
- transporter des données

De fortes disparités entre les types de collectivité

Les communes (61%) et les conseils départementaux et régionaux (50%)

CONTRE SEULEMENT

38% pour les communautés d'agglo, urbaines et métropoles et 25% pour les communautés de communes

✓ Quels usages ?

- Chiffrement des données 84% +65 pts
- Authenticité de l'information 65% +42 pts
- Authentification des utilisateurs 60% +36 pts
- Non-répudiation d'une action 20% +15 pts

La SSI dans les collectivités

✓ Et la sécurité physique ?

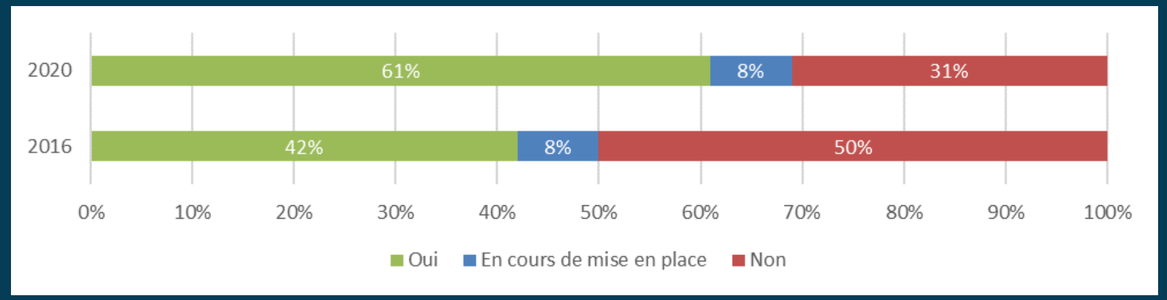
Les contrôles d'accès et la vidéoprotection en très nette progression

67% des salles machines protégées par contrôle d'accès principalement par badge

MAIS AUSSI

Renforcé par un contrôle d'accès physique et des caméras

Les communes restent moins bien dotées



Sécurisation de l'accès aux salles machines

La SSI dans les collectivités

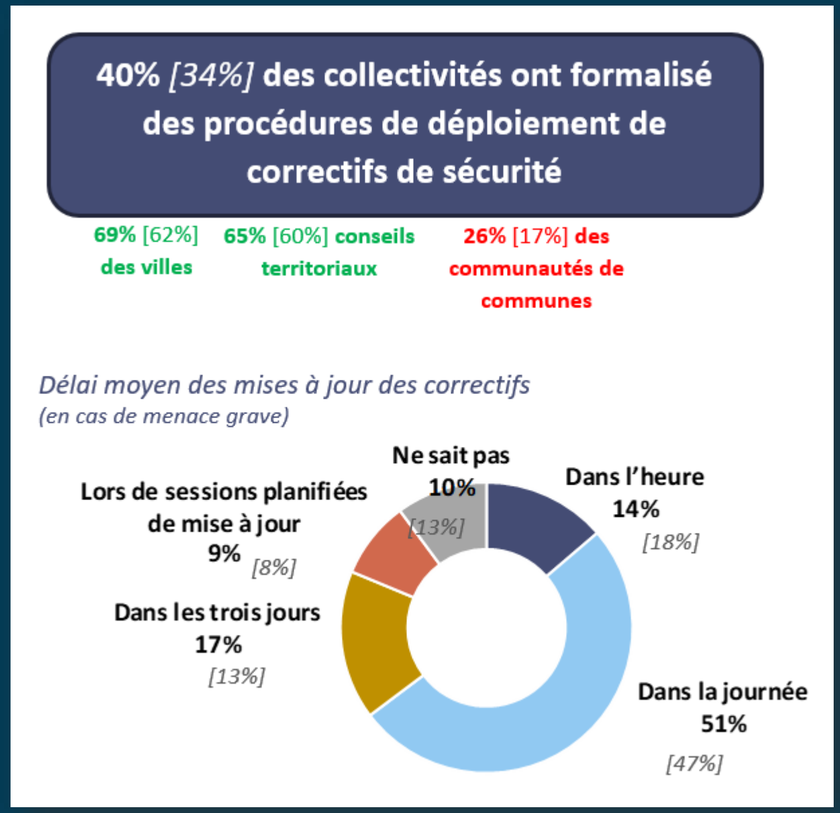
✓ L'exploitation sécurisée ?

Une première barrière est en place constituée de différentes solutions

MAIS

Encore trop de retard dans la détection et la protection

Des faiblesses aussi dans la gestion des vulnérabilités techniques et le déploiement de correctifs qui n'est formalisé que dans 40% des collectivités



La SSI dans les collectivités

✓ Ouverture sur l'extérieur

83% autorisent un accès au SI depuis l'extérieur sur un poste maitrisé +9pts

75% autorisent un accès à partir de smartphones et tablettes fournies par la collectivité +9pts

Messagerie instantanée (79%) et réseaux sociaux (86%) de plus en plus tolérés

39% autorisent un accès à Internet sans filtrage

✓ Méfiance sur le BYOD

33% autorisent un accès au SI depuis l'extérieur sur un poste non maitrisé -7pts

31% autorisent un accès à partir de smartphones et tablettes personnelles -13pts

La SSI dans les collectivités

✓ Security by default ?

Solutions sur étagère ou prestations de développement

CAR

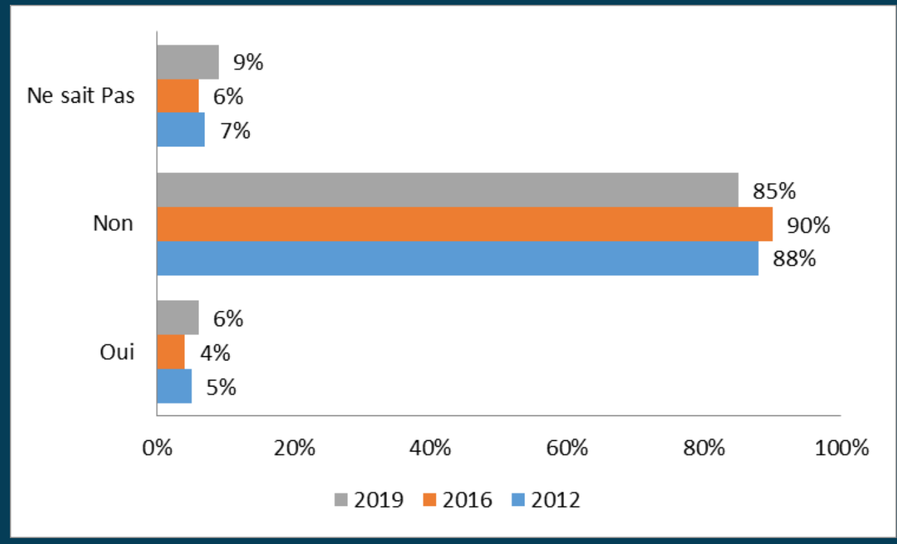
Peu de compétences en développement

CONSEQUENCE

Exigences minimalistes dans les cahiers des charges

AGRAVE PAR

L'absence de référent sécurité pour les développements



Cycle de développement sécurisé

La SSI dans les collectivités

✓ Relation avec les fournisseurs

60% des collectivités recourent à l'externalisation dont 43% en partie et 17% en totalité

La taille de la collectivité ayant un impact sur le taux d'externalisation

Des audits plus fréquents (51%) sur les fournisseurs mais pas par des indicateurs

✓ Et le cloud ?

62% des collectivités y ont recours +43pts entre 2012 et 2020

Une progression d'usage plus rapide que son encadrement !

Dans 24% des cas il est utilisé sans contrôle de la DSI ou du RSSI

Dans 79% des cas, absence de politique Cloud

La SSI dans les collectivités

CLUSIF

✓ Gestion des incidents

L'arrivée des rançongiciels avec 30% des conseils territoriaux et des villes impactés

400k€ c'est le montant de l'impact financier subi par une des collectivités ayant répondu

Pour autant le risque reste sous évalué avec 62% des répondants estimant qu'il est faible car pour 79% les données ont pu être récupérées !

53% ne communiquent pas sur les attaques par rançongiciels subies et 10% déposent plainte

✓ Et la capitalisation ?

C'est le MCO qui domine dans le traitement d'un incident et pour 68% des collectivités, il n'y a pas de cellule de collecte et de traitement des incidents !

Une situation encore pire pour les SCADA pour qui seulement 11% des cellules de collecte adresse ce type de système

38% ignorent l'impact sur la production et 80% ne procèdent pas à l'évaluation de l'impact financier d'un incident

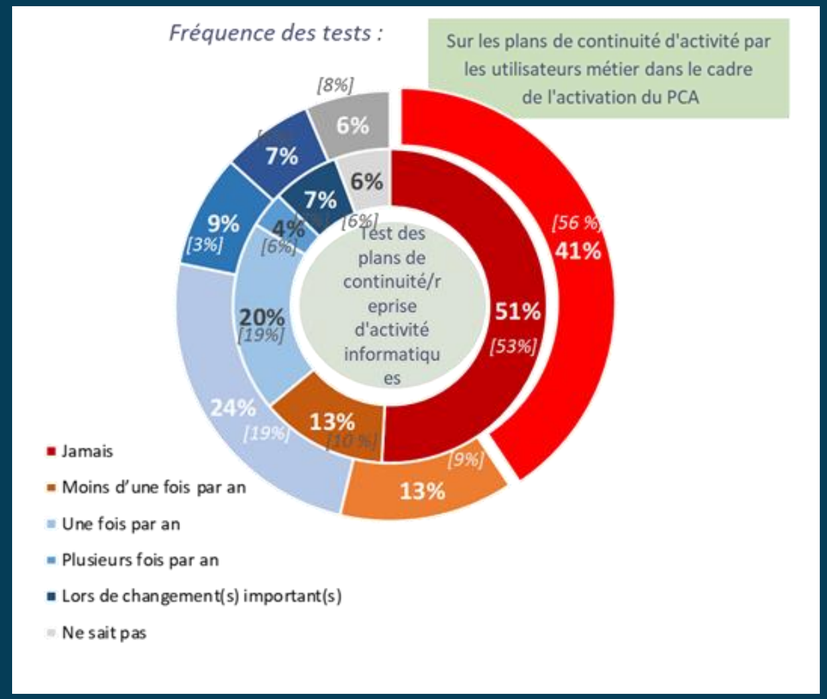
La SSI dans les collectivités

✓ PCA/PRA

¾ des collectivités ne disposent pas d'un plan de gestion de crise formalisé

Moins de 30% ont évalué les exigences métiers dans le cadre d'un BIA formel

Des PCA testés au moins une fois par an pour ¼ des collectivités



Fréquence des tests

La SSI dans les collectivités

CLUSIF

✓ Conformité règlementaire

93% des collectivités estiment être en conformité avec le RGPD

75% ont désigné un DPO, 10% en cours de désignation

Les communautés d'agglo propose souvent un DPO mutualisé aux communes associées

Il est majoritairement rattaché au DGS (51%) ou externalisé (19%) .

Par contre la conformité au RGS est plus faible avec seulement 78%

✓ Comment vérifier ?

Les audits sont :

- de plus en plus utilisés (56% bi-annuel)
- mieux connus dans leurs typologie
- motivés par les exigences règlementaires 51% ou la PSSI 31% mais aussi par les incidents 23%

Mais encore pas assez capitalisés dans des tableaux de bord de sécurité 13% seulement !

La SSI dans les collectivités

Conclusion

La SSI reste très variable entre les collectivités

Le RGPD a aidé à la prise en considération

Le RSSI encore trop souvent en juge et partie dans la DSI

Des lacunes dans la détection et la gestion des incidents

Conclusion

Globalement la situation s'améliore par rapport à l'étude précédente,

Les collectivités doivent faire en sorte que la cybersécurité ne soit plus perçue comme un frein

MAIS PLUTÔT

comme un gage de confiance dans l'usage des moyens numériques mis à dispositions des citoyens.