# Sécurité économique territoriale

## Auvergne - Rhône-Alpes

Quelle que soit l'entité (*entreprise, institution, professions libérales, …*), son organisation repose sur l'informatique.

Projets, contrats, propositions commerciales, virements, factures, plannings, échanges avec les clients, dossiers, sont autant de fichiers plus ou moins confidentiels utilisés au quotidien et échangés numériquement (*courriels, SMS, réseaux sociaux, etc*).

Si l'informatique est devenue incontournable, mal maîtrisée, elle peut être source d'importantes vulnérabilités face à des cybercriminels déterminés et très pro-actifs (*vol de données, intrusion et/ou blocage de vos systèmes avec ou sans demande de rançon, détournements d'actifs financiers, etc*).

Du moment que vous détenez et utilisez un ***smartphone***, une ***tablette***, un ***ordinateur fixe*** ou ***portable***, vous êtes une victime potentielle. **Il faut cesser de croire que ça n'arrive qu'aux autres**. Le plus important n'est pas de savoir ***SI*** vous allez être victime de la cybercriminalité mais surtout ***QUAND*** vous le serez.

**Protéger vos *avoirs immatériels* et vos *systèmes d'information* doit donc être votre *priorité*.**

## La région de gendarmerie de Rhône-Alpes et la « *sécurité économique* »

La « ***Sécurité Économique Territoriale*** » se définit comme l'ensemble des moyens actifs et passifs mis en œuvre pour assurer la ***protection du patrimoine matériel & immatériel*** d'une entreprise.

Basé sur la prévention et le conseil, le dispositif mis en œuvre par la région de gendarmerie Auvergne - Rhône-Alpes est modulable. Il vise à s'adapter à la taille et au secteur d'activité de l'entreprise, en proposant une offre allant de la simple sensibilisation au pré-diagnostic de sécurité plus élaboré.

Il s'agit d'une démarche ***non-contraignante*****,** s'adressant aux **entreprises implantées en zone de compétence de la gendarmerie nationale et basée exclusivement sur l'adhésion du dirigeant.**

## Nos 4 principales actions

**1 - Des conférences gratuites généralistes ou thématiques** (*escroqueries financières, cybercriminalité, protection de l'information, etc*).

**2 - Des plaquettes d'information et/ou de prévention, des messages d'alerte**, sur des problématiques de sûreté/sécurité récurrentes (*vol de fret, escroquerie au virement, salons professionnels, journées portes ouvertes, alertes cyber, etc*).

**3 - Le dispositif « Opération Tranquillité Entreprise »**, visant à renforcer la protection des sociétés par le biais de rondes de surveillance autour des établissements ayant signalé une problématique particulière (*fermeture pour vacances, réception de matériaux coûteux, etc*).

**4 - Le pré-diagnostic de sécurité**, permettant de réaliser une image à l'instant " ***T*** " de la sécurité/sûreté au sein de votre établissement. Lors de la restitution, les conseils formulés dans le rapport vous donneront des pistes de réflexion pour mieux sécuriser votre établissement.

***N'hésitez donc pas à faire appel à la Gendarmerie, c'est simple et gratuit !***


*Coordonnées du référent régional à la sécurité économique*

***MDL/Chef Eric POZZI***

***: 06.25.83.34.43***

***: eric.pozzi@gendarmerie.interieur.gouv.fr***

***: https://fr.linkedin.com/in/eric-pozzi-2b22a01a***


Région de gendarmerie Auvergne-Rhône-Alpes

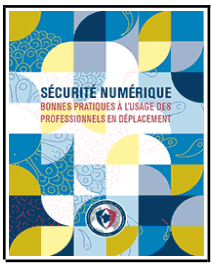
Région de gendarmerie Auvergne-Rhône-Alpes

# POUR VOUS AIDER

## 1 - Les guides


**La sécurité économique au quotidien en 26 fiches thématiques**

*lien* : https://sisse.entreprises.gouv.fr/fr/outils/la-securite-economique-au-quotidien-26-fiches-thematiques

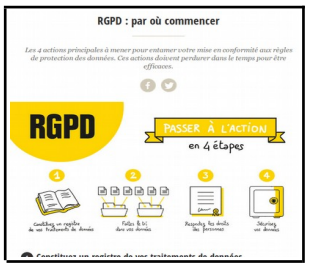




**Guides pratiques de l'ANSSI**

*lien* : https://www.ssi.gouv.fr/administration/bonnes-pratiques/

*De nombreux autres guides sont également disponibles sur ce site.*




**Le RGPD**

lien : https://www.cnil.fr/fr/rgpd-par-ou-commencer

*Visitez régulièrement le site de la CNIL*

## 2 - La sensibilisation en interne


**Kit de sensibilisation à la cybersécurité**

*lien* : https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/


**Mooc de formation de l'ANSSI**

*lien* : https://www.secnumacademie.gouv.fr/


**RGPD : Mooc de la CNIL**

*lien* : https://atelier-rgpd.cnil.fr/

# RETOUR SUR LA CONFÉRENCE À LAQUELLE VOUS AVEZ ASSISTÉ

***La sécurité informatique est primordiale pour toute entreprise et le sera de plus en plus avec l'augmentation des connexions informatiques et la dématérialisation. La menace est permanente et pèse sur tout établissement, quelle que soit sa taille ou son secteur d'activité.***

***Les risques sont nombreux et variés :***

- ✔ Vols de données sensibles (*fiches clients, projets en cours, contrats, …*).
- ✔ Perte de contrôle des systèmes d'information.
- ✔ Arrêt ou dégradation des installations.
- ✔ Escroquerie et déstabilisation.

***Les conséquences :***

- Pertes économiques et financières.
- Altérations ou pertes de données.
- Indisponibilité des services.
- Altération de l'image de l'entreprise et perte de confiance des clients, partenaires et salariés.

***Les atteintes les plus fréquentes :***

- ❍ ***Le « défacement »*** ou « ***défaçage*** » de sites internet (*remplacement de la page d'accueil originale par une autre (revendication de groupes de pressions ou terroristes*).
- ❍ ***Le phishing*** (*mails frauduleux annonçant un gain ou une démarche administrative à réaliser en ligne en vue d'obtenir des informations personnelles et/ou bancaires*).
- ❍ ***L'escroquerie au faux président*** (*ou faux ordre de virement international*).
- ❍ ***Les escroquerie au changement de domiciliation bancaire*** (*ou dite au faux RIB, …*).
- ❍ ***Les ransomwares*** (*ou rançongiciels*), logiciel malveillants incrémentés dans des pièces jointes transmises par mails. Une fois activé suite à l'ouverture de la pièce jointe, ce type de Malware chiffre l'ensemble des données contenues dans le disque dur de la machine, les périphériques reliés aux ports USB et peut même remonter sur les réseaux par le biais des fichiers partagés.

***Les bonnes pratiques pour « tenter » de se prémunir :***

- ❍ Choisir avec soin ses mots de passe (*mélange de 12 à 17 caractères différents (chiffres, lettres majuscules, minuscules, caractères spéciaux… sans lien avec l'utilisateur. Ne pas les enregistrer sur le gestionnaire de mots de passe. Avoir un mot de passe par utilisation et les changer régulièrement – Utilisation de coffres-forts à mots de passe tels Dashlane ou Keepass*).
- ❍ Être prudent lors de l'utilisation des tablettes et smartphones.
- ❍ Lors des déplacements professionnels en train, en avion, dans les hôtels, protéger les données. N'emmener que les informations nécessaires à la mission du moment, ne pas utiliser le wi-fi public (*préférer le partage de connexion avec votre smartphone ou une clé 4G*).
- ❍ Être vigilant lors des demandes de virements bancaires. En cas de doute, ne pas hésiter à faire un contre-appel de sécurité à la banque et/ou au demandeur (*si possible depuis un téléphone portable*).
- ❍ Séparer les usages personnels des usages professionnels lors de l'utilisation du matériel informatique.
- ❍ Être vigilant quant à la diffusion d'informations professionnelles ou personnelles sur internet (*penser à lancer régulièrement des recherches sur son « **prénom / Nom** » et sur son « **entreprise** » pour déceler le plus rapidement possible des problèmes pouvant porter atteinte à sa réputation*).
- ❍ Ne jamais mettre l'organigramme de l'entreprise ou d'informations sensibles sur votre site internet.
- ❍ Installer des logiciels de sécurité et les maintenir à jour.
- ❍ Effectuer quotidiennement des sauvegardes et en vérifier périodiquement leur viabilité.
- ❍ Sécuriser l'accès au wi-fi de l'entreprise (*accès utilisateurs / accès visiteurs*).
- ❍ Mettre en œuvre une charte informatique, laquelle doit avoir des vertus pédagogiques, doit expliquer les droits et les devoirs de chacun et doit mentionner les sanctions en cas de non-respect des règles édictées.
- ❍ Sensibiliser régulièrement l'ensemble des collaborateurs.

***Que faire en cas d'incident ?***

- ➢ ***Isoler rapidement les ordinateurs infectés*** (*ôter le câble Ethernet et couper wi-fi et Bluetooth pour empêcher la progression du malware*).
- ➢ ***Faire intervenir l'informaticien de l'entreprise*** ou un prestataire extérieur.
- ➢ ***Copier les données frauduleuses*** avant toute réinstallation.
- ➢ ***Déposer rapidement plainte*** auprès du service de police ou de gendarmerie territorialement compétent.
- ➢ ***Alerter votre assureur*** (*contrat cyber*).