

MES AIDES

MesServicesCyber

C'est une plateforme pour faciliter l'accès de tous aux services et ressources de l'ANSSI. Elle est conçue comme un catalogue qui permet d'accéder directement à diverses ressources utiles pour renforcer ses connaissances en cybersécurité et mieux protéger les systèmes d'informations de sa structure.

<https://messervices.cyber.gouv.fr/>

Un premier diagnostic gratuit accompagné

d'un aidant cyber est proposé sur le lien :
<https://messervices.cyber.gouv.fr/cyberdepart>

Diag Cybersecurité

C'est un dispositif du plan Cyber PME porté par la Direction Générale des Entreprises, avec le soutien de France 2030. Le Diag Cybersécurité vous permet de dresser un état des lieux de l'exposition de l'entreprise aux risques cyber. Avec un expert habilité par Bpifrance, vous disposerez d'un plan d'action priorisé afin de mieux protéger votre entreprise.

<https://www.bpifrance.fr/catalogue-offres/diagnostic-cybersecurite>

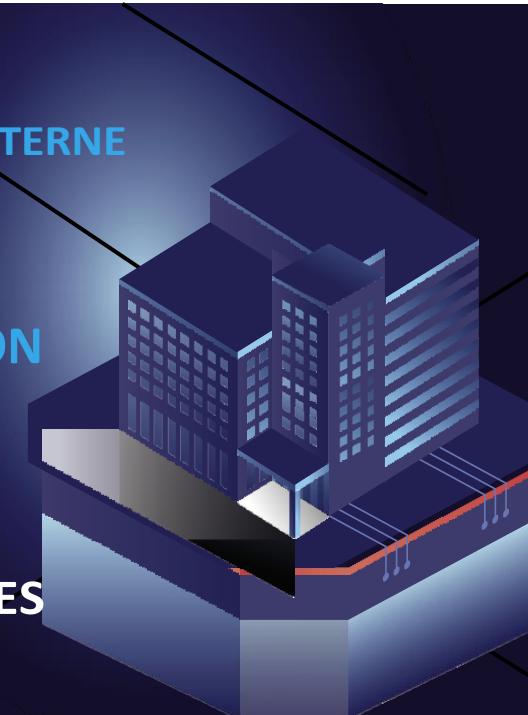


SÉCURITÉ INTERNE

PROTECTION
DU SITE

SÉCURISATION DES
FLUX

PROTECTION
DES DONNÉES



MINI-GUIDE
PRATIQUE

INTRUSION

PHISHING

CYBER
MALVEILLANCE

ESCOQUERIE

L'État s'engage pour
la sécurité économique
des entreprises



PRÉFET
DU VAL-D'OISE

Liberté
Égalité
Fraternité



Je me mobilise pour ma stratégie

Mes contacts au sein de l'État

Le Référent sécurité économique de la préfecture

Sous l'autorité du préfet de département, il est responsable, en lien avec l'échelon régional, de la mise en œuvre de la politique publique de sécurité économique.

✉ pref-securite-economique95@val-doise.gouv.fr

Le Délégué à l'information stratégique et à la sécurité économiques (DISSE)

Il est le prolongement territorial du service de l'information stratégique et de la sécurité économiques (SISSE) au niveau local. Il coordonne la détection des alertes en matière de sécurité économique et organise des actions de sensibilisation

✉ drieets-idf.disse@drieets.gouv.fr

Le Délégué de l'ANSSI en Ile-de-France

Spécialiste de la sécurité du numérique, il agit pour prévenir les incidents et sensibiliser les acteurs locaux du public et du privé à la réglementation et aux bonnes pratiques.

✉ ile-de-France@ssi.gouv.fr

La Sécurité intérieure

C'est le service de référence pour les menaces et ingérences étrangères pouvant porter atteinte au patrimoine économique, industriel et scientifique national, à la souveraineté de l'Etat ou aux intérêts fondamentaux de la Nation (hors sphère Défense).

✉ icergy95@interieur.gouv.fr

La Direction du renseignement et de sécurité de la Défense (DRSD)

Service de renseignement du ministre des Armées chargé de renseigner pour protéger les capacités de la défense nationale tant sur les forces armées, l'industrie de défense que le potentiel scientifique et technique de la Nation.

✉ drsd-dsezp-4.cds.fct@intradef.gouv.fr

La Gendarmerie nationale

L'Officier adjoint renseignement (OAR) du groupement de la gendarmerie accompagne les acteurs économiques départementaux pour diffuser une culture de sécurité du patrimoine, protéger et recueillir les renseignements d'intérêt économique, identifier et analyser les risques et menaces.

✉ cr.corg.ggd95@gendarmerie.interieur.gouv.fr

La Police nationale

Les référents « sécurité économique » du Service Départemental du Renseignement Territorial sensibilisent les entreprises aux risques après détection des vulnérabilités d'initiative ou sur demande.

✉ dipn95-rt-securite-economique@interieur.gouv.fr

La Douane

Elle vous accompagne pour construire vos projets à l'international (réglementation, accords de libre-échange, simplifications, facilitations...).

✉ pae-paris-ouest@douane.finances.gouv.fr



J'anticipe en me protégeant

Protection du site, de l'organisation, de la structure

Je n'ai pas identifié mes informations stratégiques et les risques et menaces qui pèsent sur l'entreprise. L'entreprise ne dispose pas d'une documentation générale sur sa sécurité (objectifs, organisation, moyens, procédures de mise à jour...). La sécurité n'est pas abordée dans le cadre d'un projet « politique de sécurité ».

Je contacte

> La gendarmerie : cr.corg.ggd95@gendarmerie.interieur.gouv.fr

> La police nationale : dipn95-rt-securite-economique@interieur.gouv.fr

Je réalise un diagnostic : <https://diagseco.finances.gouv.fr/home>

Protection des données et des actifs immatériels

Mes données sensibles ne sont pas protégées. En partageant certaines informations (innovations, travaux de R&D, orientations stratégiques, plans marketing...), l'entreprise accroît potentiellement sa vulnérabilité. Il est impératif de concilier la nécessité d'exposer des informations, et l'obligation de protéger certaines d'entre elles en fonction de leur niveau de sensibilité.

Je contacte

> L'ANSSI : ile-de-France@ssi.gouv.fr

> DISSE : drieets-idf.disse@drieets.gouv.fr

Je m'informe

> L'ANSSI : <https://messervices.cyber.gouv.fr/> ou <https://cyber.gouv.fr/>

> Cybermalveillance.gouv.fr : <https://www.cybermalveillance.gouv.fr/>

> INPI : <https://www.inpi.fr/fr>

> Douane : <https://www.douane.gouv.fr/demande/deposer-une-demande-d-intervention-aupres-des-services-douaniers>

> SISSE : <https://www.entreprises.gouv.fr/la-dge/publications/la-securite-economique-en-28-fiches-thematiques>

> La DRSD : drsd-dsezp-4.cds.fct@intradef.gouv.fr

Sécurisation des flux

Vos échanges internationaux sont importants. Vous souhaitez faciliter et sécuriser la chaîne logistique internationale, lutter contre la fraude. Vous travaillez ou pouvez travailler sur des marchés de défense.

Je contacte

> La Douane : pae-paris-ouest@douane.finances.gouv.fr

En complément du dépôt d'un titre de propriété intellectuelle (marque, dessin et modèle, brevet, IG, etc.) vous pouvez mettre en place une demande d'intervention qui permettra à la douane d'agir contre les produits contrefaisants en votre nom. Le statut d'OEA (Opérateur Économique Agréé) vous permettra de sécuriser vos flux (contact : Pôle d'Action Économique).



Je réagis à une attaque ou une menace

Si je subis une attaque informatique, je dois :

- > déconnecter les supports de sauvegarde,
- > ne pas éteindre les équipements infectés mais les isoler du réseau,
- > signaler l'incident à mon responsable informatique,
- > ne pas payer de rançon,
- > déposer plainte auprès des forces de Police ou Gendarmerie,
- > signaler les faits à mon assureur,
- > communiquer en interne, aux tiers susceptibles d'être impactés.

Je contacte

> CERT-FR : <https://www.cert.ssi.gouv.fr/>

✉ cert-fr@ssi.gouv.fr

① 32 18

La plateforme Cybermalveillance pour signaler les faits :

<https://www.cybermalveillance.gouv.fr>

> Urgence Cyber Ile de France : <https://urgencecyber.iledefrance.fr/>

La plateforme No More Ransom, en cas de rançongiciel :

<https://www.nomoreransom.org/fr/index.html>

Si je subis une intrusion, désorganisation ou une manipulation et escroquerie, je dois :

- > vérifier et confirmer l'identité de l'interlocuteur,
- > procéder à un contre appel téléphonique,
- > signaler les comportements inhabituels et/ou sollicitations d'urgence au N+1, prévenir le responsable sécurité de l'entreprise ou le commissariat de police ou la gendarmerie,
- > vérifier par rapport aux seuils et aux fréquences de virement fixés par le DAF si transfert de fonds à l'étranger, je contacte immédiatement ma banque,
- > mettre en œuvre une veille adaptée.

Je contacte

> Pour les faits consommés ou tentatives, déposer plainte à la gendarmerie ou la police nationale.

J'ai des doutes sur un partenaire, un client ou un investisseur potentiel. Que faire ?

- > vérifier l'identité de l'interlocuteur et confirmer ses intentions,
- > s'assurer de son honabilité par une « due diligence »,
- > maîtriser sa communication en ne transmettant aucune information stratégique avant la signature d'un accord de confidentialité,
- > mettre en œuvre une veille adaptée.

Je contacte

> Le DISSE : drieets-idf.disse@drieets.gouv.fr