

Comment se préparer aux incidents de sécurité ?

 <p>Denis JACOPINI</p> <p>UNE CARTE BANCAIRE ANTI-FRAUDE ?</p> <p>vous informe</p> <p>LCI</p>	<p>Comment se préparer aux incidents de sécurité ?</p>
--	--

Les entreprises doivent être prêtes à agir face à des incidents de sécurité et à des attaques. Et cela passe notamment par sept points précis (par Peter Sullivan).

Un plan de préparation à la cybersécurité présente et détaille les objectifs fondamentaux que l'organisation doit atteindre pour se considérer comme prête à faire face à des incidents de sécurité informatique. La liste de contrôles qui va suivre n'est pas exhaustive, mais elle souligne des objectifs qui constituent un minimum requis pour donner un niveau raisonnable de sensibilisation à la cybersécurité et se concentrer sur la protection des actifs informationnels essentiels.

Ici, la préparation à la cybersécurité est définie comme l'état permettant de détecter et de réagir efficacement aux brèches et aux intrusions informatiques, aux attaques de logiciels malveillants, aux attaques par hameçonnage, au vol de données et aux atteintes à la propriété intellectuelle – tant à l'extérieur qu'à l'intérieur du réseau.

Un élément essentiel de cette définition est de « pouvoir détecter ». La détection est un domaine où une amélioration significative peut être atteinte en abaissant le délai de détection, couramment observé entre 9 et 18 mois. Une capacité de détection plus rapide permet de limiter les dommages causés par une intrusion et de réduire le coût de récupération de cette intrusion. Être capable de comprendre les activités régulières du réseau et de détecter ce qui diverge de la norme est un élément important de la préparation à la cybersécurité. Voici une sept objectifs que les entreprises devraient considérer.

Les objectifs à atteindre

1. Plan de cybersécurité

2. Gestion du risque

3. Gestion de l'identité

- Contrôle d'accès
- Authentification
- Autorisation
- Responsabilité

4. Surveillance de réseau

5. Architecture de sécurité

6. Contrôle des actifs, des configurations et des changements

7. Cartographie de la gestion des incidents

...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus

d'informations

sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Se préparer aux incidents de sécurité*

Un baccalauréat en cybersécurité à Polytechnique Montréal



Un
baccalauréat
en
cybersécurité
à
Polytechnique
Montréal

La Commission des études a approuvé la création d'un nouveau baccalauréat en cybersécurité qui sera offert à Polytechnique Montréal à l'automne 2017.

Les demandes pour un programme de formation en ligne en cybercriminalité, incluant des stages en entreprise, se sont faites pressantes au cours des dernières années et Polytechnique Montréal a décidé de créer un baccalauréat par cumul avec appellation en cybersécurité. La Commission des études de l'Université de Montréal a donné son approbation à ce projet à sa réunion du 21 mars.

Le nouveau programme permettra de combiner deux certificats liés à la thématique (cyberenquête, cyberfraude ou cybersécurité) avec un autre programme de 30 crédits de l'UdeM ou de HEC Montréal en vue de l'obtention d'un diplôme de baccalauréat. L'école de génie, rappellent les responsables, offre une formation en cybersécurité au premier cycle depuis 2007. Le projet vise à répondre «le plus adéquatement possible aux nouveaux besoins du marché du travail, qui est confronté à une pénurie de main-d'œuvre amplifiée par un taux de cybercriminalité en hausse exponentielle. De plus, la multiplication des supports mobiles ainsi que l'émergence de l'infonuagique posent de nouveaux défis».

Considérant qu'une proportion importante des étudiants de ces programmes ne possèdent pas de diplôme universitaire de premier cycle, et considérant le manque de main-d'œuvre dans ces domaines, «il apparaît essentiel que le diplôme de baccalauréat qui pourrait être décerné par cumul de certificats présente une dénomination spécifique [du] domaine d'études et de pratique, dans une perspective de valeur ajoutée, tant pour la formation que pour l'employabilité et la reconnaissance des entreprises qui emploient ces diplômés», fait valoir Polytechnique Montréal.

Le nouveau programme devrait voir le jour l'automne prochain.

(MATHIEU-ROBERT SAUVÉ)

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DIREF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.





[Contactez-nous](#)

Réagissez à cet article

Source : *Un baccalauréat en cybersécurité à Polytechnique Montréal* | UdeMNouvelles

Cnil : méthode pour la mise en conformité et la prise en compte de la vie privée | Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p>  <p>vous informe...</p>	<p>Cnil : méthode pour la mise en conformité et la prise en compte de la vie privée</p>
---	--

La Commission (Cnil) a publié, il y a peu, sa méthode pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits afin de mener des PIA (Privacy Impact Assessment).

Dans un communiqué du 2 juillet 2015, la Commission nationale de l'informatique et des libertés (Cnil) a publiée une méthode pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits afin de mener des PIA (Privacy Impact Assessment).

Cette méthode qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la Cnil.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

- les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés, et ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
- la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.

Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :

- étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
- étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
- étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
- validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

<http://www.lemondedudroit.fr/droit-a-entreprises/technologies-de-linformatique/208258-cnil-methode-pour-la-mise-en-conformite-et-la-prise-en-compte-de-la-vie-privee.html>

Votre responsabilité engagée en cas de piratage de vos données | Denis JACOPINI



**Votre
responsabilité
engagée en
cas de piratage de
vos données**

Si vous vous faites pirater votre ordinateur ou votre téléphone, votre responsabilité pourrait bien être engagée vis-à-vis des données que ce support numérique renferme.

Imaginez que vous disposez de différents appareils numériques informatiques renfermant une multitude de données, dont des données d'avis, de prospects, de clients, de fournisseurs (tout ce qu'il y a de plus normal), et tout à coup, à cause d'un malware (maliciel selon D. JACOPINI), un pirate informatique en prend possession de ces données, les utilise ou pire, les diffuse sur la toile. Que risquez-vous ?

En tant que particulier victime, pas grand chose, sauf s'il est prouvé que votre négligence est volontaire et l'intention de nuire retenue.

Par contre, en tant que professionnel, en plus d'être victime de piratage (intrusion causée par une faille, un virus, un cryptovirus, un bot, un spyware), et d'avoir à assumer les conséquences techniques d'un tel acte illicite pourtant pénalement sanctionné notamment au travers de la loi godfrain du 5 janvier 1988 (première loi française réprimant les actes de criminalité informatique et de piratage), vous risquez bien de vous prendre une seconde claque vis à vis de la loi Informatique et Libertés du 6 janvier 1978.

En effet, les entreprises, les sociétés, tous ceux exerçant une activité professionnelle réglementée ou non, les associations, les institutions, administrations et les collectivités, sont tenues de respecter la loi Informatique et Libertés du 6 janvier 1978 et notamment la sécurité des données selon les termes de son Article n°34 :

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

De plus, les sanctions jusqu'alors limitées à 5 ans d'emprisonnement et 300 000 euros d'amendes vont à partir du 25 mai 2018, par la mise en application du RGPD (Règlement Général sur la Protection des Données) être portées à 20 millions d'euros et 4% du chiffre d'affaire mondial.

Partons d'un cas concret.

La société Cochabonardais voit son système informatique piraté. Des investigations sont menées et le pirate informatique arrêté.

Vis à vis de la loi Godfrain du 5 janvier 1988, le voyou risque jusqu'à 2 ans de prison et 20 000 euros d'amende. Or ce dernier, après avoir découvert que la société Cochabonardais n'était pas en règle avec la CNIL la dénonça auprès de cette dernière.

Le responsable de traitement, appréhendé le chef d'entreprise risquera, lui, 5 ans de prison et 300 000 euros d'amende, une peine bien supérieure à son voleur.

Est-ce bien normal ?

Non, mais pourtant c'est comme ça et ça peut être le cas de toutes les entreprises, administrations et administrations françaises en cas de piratage de leurs ordinateurs, téléphones, boîtes e-mail.

Autre cas concret

Monsieur Roudbou-Maitout voit son téléphone portable mal protégé et exposé aux virus et aux pirates. Un jour il apprend par un ami que les contacts de son téléphone se sont fait pirater. Il se déplace à la Police ou à la Gendarmerie, dépose une plainte mais le voleur n'est jamais retrouvé. Qui est responsable de cette fuite d'informations ?

La première chose à savoir, c'est si ce téléphone est professionnel ou personnel. S'il est professionnel, réfère vous au cas concret précédent. Si par contre le téléphone portable est personnel, les particuliers ne sont pour l'instant pas concernés par l'obligation de sécurisation des données.


Ainsi, si la faute volontaire du propriétaire de l'appareil n'est pas retenue, le seul responsable de cette fuite de données sera et restera l'auteur du piratage.

Denis JACOPINI est Expert Informatique et aussi formateur en Protection des données personnelles (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 04 62042 04).

Nous pouvons vous assister des actions de sensibilisation ou de formation à la Protection des Données Personnelles, au risque informatique, à l'hygiène informatique et à la mise en conformité après de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.le-net-expert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles>

Denis JACOPINI



Denis JACOPINI est Expert Informatique spécialisé en cybersécurité et protection des données personnelles.


- Expertises techniques (logs, réseaux, appareils, logiciels, systèmes d'exploits...) et analyses forensiques (ordinateurs, tablettes, smartphones, serveurs...)
- Exploitation de vulnérabilités de sécurité (Red/Blue Team)
- Formations et conférences en cybersécurité
- Membres de l'AN (Association Nationale Informatique et Sécurité)
- Accompagnement à la mise en conformité CNIL et en RGPD

Le Net Expert
INFORMATIQUE
SOLUTIONS ET FORMATION

02 38 38 38 38

Réagissez à cet article
Original de l'article mis en page : [Informatique et Libertés : suis-je concerné ?](#) | CNIL

Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité | Denis JACOPINI



Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité

La sensibilisation et l'éducation des utilisateurs jouent un grand rôle dans la réduction des risques.

Il importe donc pour les entreprises d'encourager leurs collaborateurs à se comporter de manière cohérente, en respectant des processus et procédures communiqués clairement, dont la conception et la surveillance sont centralisées et qui couvrent la totalité des équipements en usage. Cela n'évitera peut-être pas toute tentative d'attaque mais renforcera certainement la sécurité de l'entreprise.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI et

<http://www.globalsecuritymag.fr/Les-entreprises-revoient-leur,20150826,55304.html>

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
---	---	---	---	--	--



RGPD

LeNetExpert

Mise en conformité RGPD : Accompagnement personnalisé par des Experts

Alors que les entreprises sont de plus en plus sensibilisées aux risques de failles, de mise hors service de leurs systèmes (attaques DDOS) et de destruction de leurs données (via des ransomwares), elles ne pensent pas forcément que leurs outils de communication unifiée sont également concernés par les règles de protection.

- **Le chiffrement** : toutes les données, qu'elles soient stockées ou en transmission, doivent être protégées, les premières avec au minimum un chiffrement AES 128 bits et les secondes en ajoutant au moins le protocole TLS. Point important : il faut bien évidemment que les messages de tous les interlocuteurs, externes compris, soient cryptés.
- **Le pare-feu** : attention à ne pas tomber dans le piège d'une solution qui expose des applications, des serveurs ou des équipements hors du pare-feu. De plus, il faut s'assurer que les solutions gèrent correctement le parcours des données au travers des serveurs d'authentification déjà en place.
 - **Les mises à jour** : puisque les mises à jour de firmwares et autres logicielles corrigent essentiellement des vulnérabilités ou apportent des dispositifs de sécurité plus robustes, il est primordial qu'elles se fassent de manière automatique pour s'assurer que le SI est protégé le plus tôt possible. Une des approches consiste à passer par une solution en Cloud, automatiquement mise à jour par le fournisseur lui-même **mais à manier avec précaution car si vous avez déjà opté pour le Cloud, avez-vous la certitude que seuls les utilisateurs autorisés accèdent à cet espace de stockage externalisé ? Qui peut bien se connecter pendant que vous dormez ?**
- **La sécurité physique** : où se situent les données que stocke la solution de communication ? Il est essentiel d'avoir la garantie que le datacenter du fournisseur soit protégé 24/7 et qu'il soit régulièrement audité et protégé contre les intrusions physiques.
- **Changer les paramètres par défaut** : Changer tous les identifiants et mots de passe de ceux proposés par défaut pour quelque chose de plus complexe est une règle d'or en matière de cybersécurité.

« Parmi les nombreuses cyberattaques survenues en 2016, la plus célèbre fut celle lancée par le botnet Mirai qui ciblait les webcams. Or, si cette attaque a autant réussi, c'est parce que les mots de passe administrateurs par défaut de ces équipements étaient toujours actifs », dit-il.
- **Sécuriser le réseau, jusqu'aux utilisateurs** : Un segment non sécurisé du réseau est une porte d'entrée par laquelle peuvent passer les cyber-attaques pour atteindre tout le SI d'une entreprise. Les méthodes pour sécuriser le réseau comprennent l'application de restrictions d'accès, le blocage au niveau du pare-feu de certaines pièces attachées et le test régulier des failles de sécurité connues. Mais Gustavo Villardi prévient qu'il ne s'agit là que de résoudre une partie du problème. « Selon une étude récente menée par Verizon sur les failles de sécurité, l'erreur humaine continue d'être la cause principale des cyber-attaques. Les collaborateurs sont le maillon faible et les entreprises se doivent de former leur personnel pour qu'ils restent protégés en ligne et depuis quelque appareil que ce soit », témoigne-t-il.
- **L'usage à domicile** : les collaborateurs en télétravail ne bénéficient pas de l'encadrement de la DSI pour sécuriser leur accès domestique. Il est donc nécessaire de leur indiquer comment sécuriser une box pour activer le chiffrement du Wifi et passer par un VPN.
- **Les mots de passe** : des bonnes pratiques doivent être appliquées pour que les mots de passe de chaque salarié soient impossibles à deviner ; cela comprend aussi bien de la complexité dans l'enchaînement des caractères que la fréquence de remplacement des mots de passe.
- **L'accès** : les collaborateurs devraient toujours éteindre un équipement lorsqu'ils ne s'en servent pas, afin d'éviter que quelqu'un ne se connecte sur les services restés ouverts
- **Le mode privé** : l'utilisation d'un système de visioconférence uniquement avec les paramètres du mode privé évite que quelque des personnes extérieures puissent se greffer sur une conférence.

[lire l'intégralité de l'article source]

LE NET EXPERT

:

- **FORMATIONS / SENSIBILISATION (utilisateurs / chefs d'entreprises / DSI) :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - AU RGPD
 - À LA FONCTION DE DPO
 - **MISE EN CONFORMITÉ RGPD / CNIL**
 - ÉTAT DES LIEUX RGPD de vos traitements)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - **RECHERCHE DE PREUVES (outils Gendarmerie/Police)**
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
 - **EXPERTISES & AUDITS (certifié ISO 27005)**
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »
« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- **Mises en conformité RGPD** ;
- Accompagnement à la mise en place de DPO ;
- **Formations** (et sensibilisations) à la **cybercriminalité** (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- **Recherche de preuves** téléphones, disques durs, e-mails, contenus, détournements de clientèle... ;
- **Expertises de systèmes de vote électronique** ;



Contactez-nous

Réagissez à cet article

Source : *Cybersécurité : les trois mesures à prendre pour protéger la communication unifiée – Global Security Mag Online*

Formations RGPD Protection des données personnelles et en Cybercriminalité

Parce que la Cybercriminalité et la Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment.



NOS SERVICES :

- Formations **RGPD** (Règlement Général sur la Protection des Données) ;
- Formations en **Cybercriminalité** ;
- **Sensibilisations** à la cybercriminalité ;
- **État des lieux** RGPD ;

- **Mise en conformité** RGPD ;
 - **Analyses de risques** (PIA / DPIA) ;
- **Audits sécurité** ;

VOTRE PROFIL :

- **CLUB D'ENTREPRISES, ORDRES, FÉDÉRATIONS, CORPORATION**
: Quelles sont vos responsabilités, quels sont vos risques, quelles devraient être vos priorités ? Que ça soit en matière de Protection des Données Personnelles (RGPD) ou de cybercriminalité, faisons ensemble un état des lieux. Agir sur vos équipements ? Sensibiliser votre personnel ? Libre à vous ensuite d'agir en fonctions de nos recommandations sur les points qui vous sembleront prioritaires.
- **ÉTABLISSEMENTS / CENTRES DE FORMATION / ORGANISATEURS D'ÉVÉNEMENTS** : Que ça soit en protection des données personnelles ou en Cybercriminalité, permettez à vos stagiaires de découvrir les notions essentielles ;
- **CHEFS D'ENTREPRISE / ÉQUIPE INFORMATIQUE** : Nous vous formons dans vos locaux et réalisons en collaboration avec votre équipe informatique une analyse détaillée de vos installation à la recherche de failles et d'axes d'amélioration conformément aux règles de l'art ou de la réglementation en vigueur (RGPD).

LES SUJETS DE FORMATION :



Consultez notre catalogue

COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ

Durée : 2 jours ou 4 jours (2 jours tout public + 2 jours approfondissement pour techniciens/informaticiens)

VIRUS, DEMANDES DE RANÇONS, VOL DE DONNÉES... PROTÉGEZ-VOUS !

Durée : 1 jour

LES ARNAQUES INTERNET À CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR

Durée : 1 jour

COMMENT BIEN UTILISER LE CLOUD

Durée : 1 jour

COMMENT PROTÉGER VOTRE IDENTITÉ ET VOTRE VIE PRIVÉE SUR INTERNET

Durée : 1 jour

DÉCOUVREZ 50 LOGICIELS GRATUITS À CONNAÎTRE ABSOLUMENT

Durée : 1 jour

RGPD CE QU'IL FAUT SAVOIR POUR NE PAS LE PAYER CHER

Durée : 1 jour

RGPD : ANALYSONS CE QUE VOUS AVEZ COMMENCÉ

Durée : 1 jour (il est recommandé d'avoir déjà mis en pratique une mise en conformité au moins 15 jours avant)

COMMENT BIEN UTILISER LES DONNÉES DANS LE CLOUD

Durée : 1 jour

À LA DÉCOUVERTE DU DARKNET (LE WEB CLANDESTIN)

Durée : 1 jour

DÉTECTER ET GÉRER LES CYBER-ATTAQUES

Durée : 2 jours

APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

APPRENEZ À RÉALISER DES TESTS D'INTRUSION SUR VOTRE SYSTÈME INFORMATIQUE

Durée : 2 jours

Remarque :

Un sujet peut être traité en quelques heures mais aussi en quelques jours.

Malgré un minimum de théorie à connaître, nous pouvons réaliser un mélange de ces thèmes afin de vous proposer un contenu personnalisé en fonction des thèmes et durées globales souhaités.

EN FORMAT CONFÉRENCE :

QUE NOUS RÉSERVE LA CYBERCRIMINALITÉ DANS LES 12 PROCHAINS MOIS ?

Conférence personnalisable en général sur 1h30 + 30min Questions / réponses) (Demandez le programme détaillé)

RGPD – CE QU’IL FAUT SAVOIR POUR NE PAS LE PAYER

Conférence personnalisable en général sur 1h30 + 30min Questions / réponses) (Demandez le programme détaillé)

FONCTIONNEMENT :

- Vous organisez des formations dans votre établissement ou dans des locaux adaptés : Nous pouvons animer de 1 à 6 jours de formation sur les sujets ci-dessus ;
- Vous organisez un forum ou un salon, nous pouvons préparer une conférence de 20 minutes à 1h30 ou participer à des tables rondes ;
- En faculté ou établissement scolaire, nos interventions seront de 3 à 35 heures.
- Pour une journée de formation, nos interventions sont prévues généralement prévues du mardi au jeudi (Lundi, Vendredi et Samedi sous conditions).
- Nos formations d’une journée sont prévues pour une durée de 7 heures par jour maximum.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



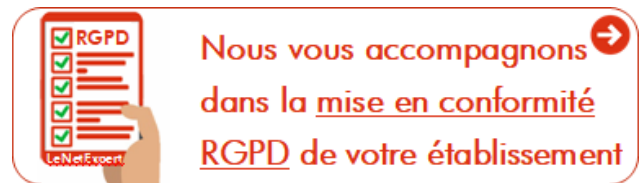
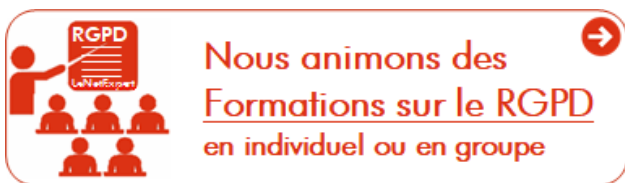
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD.**

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016


DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Dispositif biométrique d'accès à la cantine : quelles formalités à la CNIL ? | Denis JACOPINI

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<p>Dispositif biométrique d'accès à la cantine : quelles formalités à la CNIL ?</p>
---	---

Les dispositifs biométriques utilisant le contour de la main des élèves pour gérer l'accès à la cantine scolaire sont couverts par une autorisation unique adoptée par la CNIL.

Les établissements qui souhaitent installer ce type de dispositifs doivent faire une déclaration simplifiée, en sélectionnant dans l'onglet « Finalité » l'autorisation unique AU-009.

Le responsable du dispositif s'engage ainsi à se conformer aux caractéristiques décrites dans ce texte.

Les autres dispositifs biométriques (réseaux veineux, empreintes digitales, reconnaissance faciale, etc.) doivent faire l'objet d'une demande d'autorisation préalable auprès de la CNIL.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :

<http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=D5FEF7DD5664BF01E19E95AF8AF7782F>

Formation RGPD pour devenir DPO de votre organisme – Prochaine formation les 17 18 et 19 septembre 2018 à Paris

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p>	 <p>LE NET EXPERT SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
		<p>Formation RGPD pour devenir DPO de votre organisme – Prochaine formation les 17 18 et 19 septembre 2018 à Paris</p>			

Depuis le 25 mai 2018, le RGPD (Règlement européen sur La Protection des Données) est applicable. De nombreuses formalités auprès de la CNIL ont disparu. En contrepartie, la responsabilité des organismes est renforcée. Ils doivent désormais assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Formation pour DPD « Je veux devenir le Délégué à la Protection des Données de mon établissement » : 2 jours (Mettez en place une démarche de mise en conformité RGPD)

Que vous soyez bientôt ou soyez déjà désigné « Délégué à la Protection des Données » ou « DPD », nous vous conseillons cette formation. Cette formation vous permettra de rentrer en profondeur dans le Règlement Européen et vous présentera des éléments concrets afin de mettre en place durablement une mise en conformité avec le RGPD au sein de votre établissement. Consultez les prochaines dates d'animation autour de chez vous ?



Je me présente : Denis JACOPINI. Je suis Expert de justice en informatique **spécialisé en cybercriminalité et en RGPD (protection des Données à Caractère Personnel)**, consultant depuis 1996 et formateur depuis 1998. J'ai bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel. De formation d'abord technique, Correspondant CNIL (CIL : Correspondant Informatique et Libertés) puis récemment Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il m'est ainsi aisé d'expliquer le côté pragmatique de la démarche de mise en conformité avec le RGPD.

« Mon objectif est de vous transmettre mon savoir, vous dévoiler mes techniques mes outils car c'est bien ce que les personnes qui souhaitent s'inscrire à une formation RGPD attendent. »

Votre Prénom / NOM (obligatoire)

Votre adresse de messagerie (obligatoire)

Un numéro de téléphone (pour faciliter l'organisation)

Vous souhaitez avoir des informations sur :

- la formation « Comprendre le RGPD » : 1 jour
- la formation « Je veux devenir Délégué à la Protection des Données » 2 jours
- la formation « Je mets en conformité mon établissement » 3et 1 jours
- la formation « Mise en conformité RGPD sur mesure »
- un accompagnement personnalisé au RGPD

Vous souhaitez réserver une ou plusieurs place(s) à la formation :

Formation pour TPE/PME : « **Comprendre le RGPD et ce qu'il faut savoir pour bien démarrer** »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour DPD : « **Je veux devenir le Délégué à la Protection des Données de mon établissement** »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Formation pour consultants : « **J'accompagne mes clients dans leur mise en conformité avec le RGPD** »

Pas de date de prévue pour l'instant.

Face à une importante demande en formations et en accompagnements personnalisés ou individuels, nous avons momentanément interrompu l'organisation de formations de groupe. Nous sommes néanmoins à votre entière disposition si vous souhaitez organiser une formation dans vos locaux. N'hésitez pas à nous faire part de vos besoins et voyons ensemble si nous pouvons vous trouver une solution.

Autre ville ou sujets souhaités en individuel (indiquez ci-dessous)

Votre message avec vos préférences de date ou vos commentaires

Envoyer

Nos formations s'organisent en groupe. Le lieu de la formation sera facilement accessible à Métro à Paris, facilement accessible en tramway à Lyon et à proximité d'une gare TGV et disposera d'un parking à Marseille. Votre place ne sera réservée qu'à la réception de votre acompte. Si la formation était annulée (nombre de participants insuffisants ou en cas de force majeure), votre acompte sera remboursé en intégralité dans les 5 jours (les chèques seront encaissés à partir du jour de la formation). En cas d'annulation de votre part moins de 48 heures avant la formation, l'acompte pourra ne pas être remboursé car destiné à régler les frais de réservation de salle et d'organisation, eux même non remboursables.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



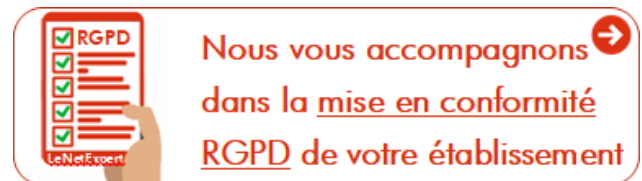
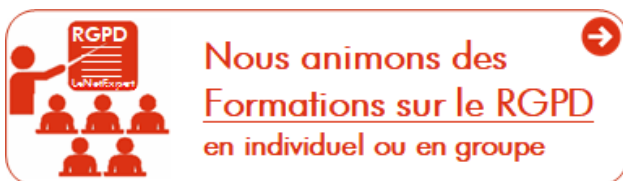
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD.**

« *Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL.* ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Source : Denis JACOPINI et *Règlement européen : se préparer en 6 étapes*