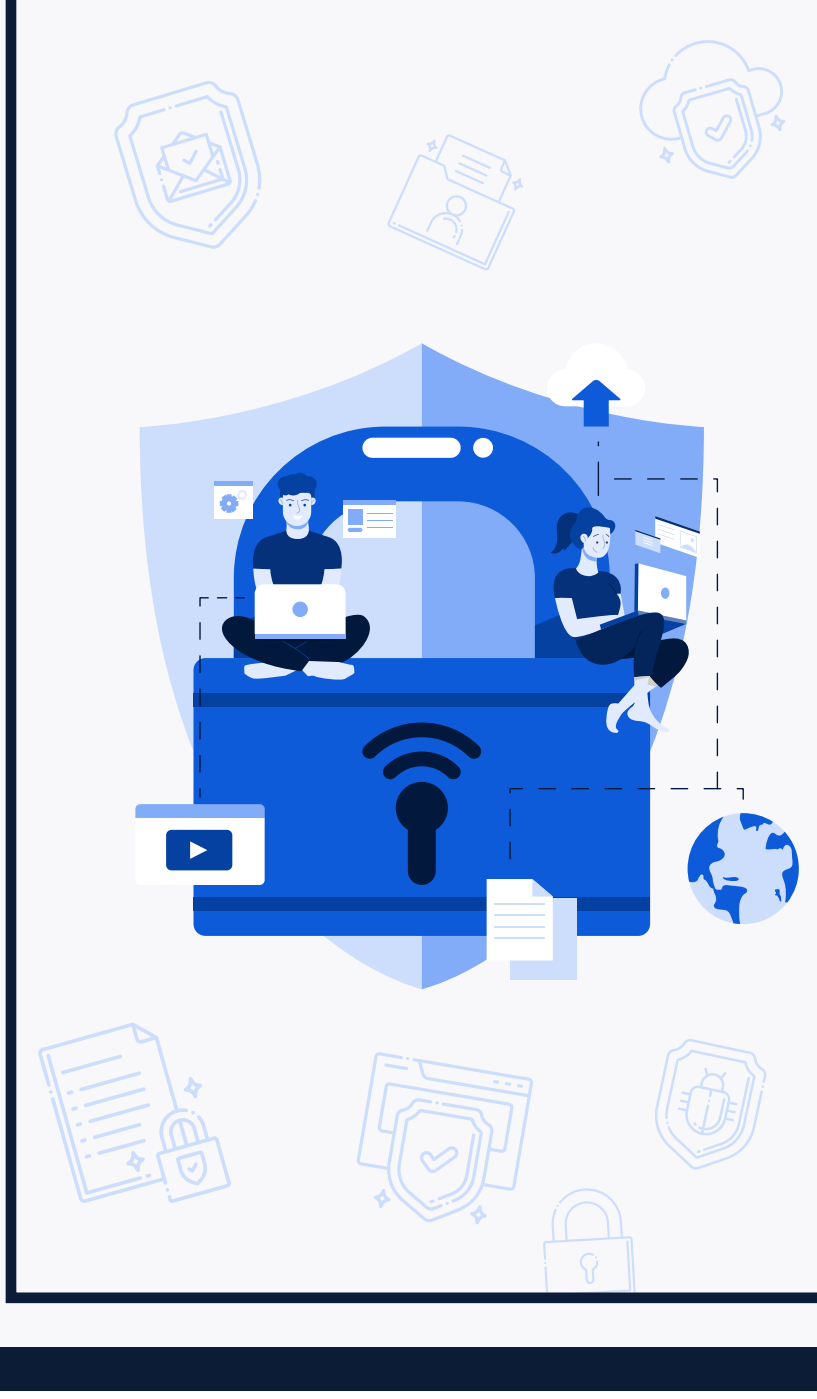
CCN-CERT

BP/01



Principes et recommandations de base en matière de Cybersécurité

RAPPORT DE LES MEILLEURES PRACTIQUES

MARS **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Édita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Centro Criptológico Nacional, 2021

Date de Sortie : mars 2021

LIMITATION DE LA RESPONSABILITÉ

Ce document est fourni conformément aux conditions qu'il contient, rejetant expressément toute garantie implicite qui pourrait y être liée. En aucun cas, le Centre National de Cryptologie ne peut être tenu responsable des dommages directs, indirects, fortuits ou extraordinaires dérivés de l'utilisation des informations et du logiciel indiqués, même s'il a été averti de cette possibilité.

AVIS JURIDIQUE

Il est strictement interdit, sans l'autorisation écrite du Centre National de Cryptologie, sous les sanctions prévues par la loi, de reproduire partiellement ou totalement ce document par quelque moyen ou procédé que ce soit, y compris la reprographie et le traitement informatique, et d'en distribuer des copies par location ou prêt public.

Index

1. **À propos de CCN-CERT** 4
2. **Introduction** 5
3. **Facteurs de menace** 6
    - 3.1 Attaques ciblées (APT) 8
4. **L'internet profond** 10
    - 4.1 Le réseau TOR 11
    - 4.2 Bitcoins 12
5. **Applications** 13
    - 5.1 Cryptage des données 15
    - 5.2 Pare-feu personnels 16
    - 5.3 Applications anti-malware 17
    - 5.4 Effacement sécurisé des données 18
6. **Une navigation sûre** 19
7. **Adresse email** 22
8. **Virtualisation** 24
9. **Sécurité des appareils mobiles** 27
10. **Sécurité des réseaux sans fil** 29
11. **Messagerie instantanéeL** 31
12. **Les réseaux sociaux** 34
13. **L'internet des objets (IoT)** 36
14. **Politique de sécurité** 39
    - 14.1 Gouvernance 43
    - 14.2 Gestion de la configuration 45
    - 14.3 Surveillance 47
    - 14.4 Politiques de continuité des affaires et de sauvegarde 49
    - 14.5. Gestion des incidents 50
15. **Décalogue de sécurité de base** 54

1. À propos de CCN-CERT

Le CCN-CERT est la capacité de réponse aux incidents de sécurité de l'information du Centre national de cryptologie.

Le CCN-CERT (www.ccn-cert.cni.es) est la capacité de réponse aux incidents de sécurité de l'information du Centre national de cryptologie, CCN (www.ccn.cni.es). Ce service a été créé en 2006 en tant que **CERT gouvernemental/national** espagnol et ses fonctions sont définies dans la loi 11/2002 réglementant le centre national d'intelligence, le RD 421/2004 réglementant le CCN et le RD 3/2010, du 8 janvier, réglementant le schéma de sécurité nationale (ENS), modifié par le RD 951/2015, du 23 octobre.

Selon eux, le CCN-CERT est responsable de la gestion des cyber-incidents affectant les **systèmes du secteur public**, les **entreprises et organisations d'intérêt stratégique pour le** pays et tout système classifié. Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à traiter activement les cybermenaces.

2. Introduction

La sensibilisation, le bon sens et les bonnes pratiques sont les meilleures défenses pour prévenir et détecter les incidents dans l'utilisation des systèmes de technologies de l'information et de la communication (TIC).

On peut dire qu'aucun Système ne garantit à 100% la sécurité du service qu'il fournit et des informations qu'il traite, en raison, dans une large mesure, des vulnérabilités présentées par les technologies et, surtout, de l'impossibilité de disposer de ressources suffisantes pour y faire face. Par conséquent, il est toujours nécessaire d'accepter un risque, celui dit résiduel, supposant un compromis entre le niveau de sécurité, les ressources disponibles et la fonctionnalité souhaitée.

La mise en œuvre de la sécurité implique une planification et la prise en compte des éléments suivants:

La sensibilisation, le bon sens et les bonnes pratiques sont les meilleures défenses.

Analyse des risques

Étudier les risques possibles et évaluer leurs conséquences sur le patrimoine. (Information et service).

Gestion des risques

Évaluer les différentes mesures de protection et décider de la solution qui convient le mieux à l'entité. (Détermination du risque résiduel).

Gouvernance

Adapter le fonctionnement normal de l'entité aux mesures de sécurité.

Vigilance

L'observation permanente des mesures de sécurité, ainsi que leur adaptation à l'émergence de nouvelles technologies.

Plans d'urgence

Détermination des mesures à adopter en cas d'incident de sécurité.

La combinaison de ces pratiques permet d'assurer le niveau de protection minimal nécessaire à la sécurité des données.

3. Facteurs de menace

La généralisation de l'utilisation des médias électroniques dans le développement normal de la société a augmenté la zone d'exposition aux attaques et, par conséquent, les bénéfices potentiels qui en découlent, ce qui constitue sans aucun doute l'une des plus grandes motivations des attaquants.

Ces dernières années, la tendance s'est poursuivie, avec une augmentation du nombre, du type et de la gravité des attaques contre les systèmes d'information du secteur public, des entreprises et des institutions d'intérêt stratégique ou disposant d'importants actifs de propriété intellectuelle et industrielle et, en général, contre tout type d'entités et de citoyens.

Les actions de **cyberespionnage** cyberespionnage sont toujours présentes. Il s'agit de cyberattaques initiées ou parrainées par des États et perpétrées par eux-mêmes ou par d'autres acteurs rémunérés, et toujours dans l'intention de s'approprier des informations sensibles ou précieuses d'un point de vue politique, stratégique, sécuritaire ou économique.

En résumé, nous pouvons dire que le cyberespionnage présente les caractéristiques générales suivantes:

- **Origine dans les États, les industries ou les entreprises.**
- **Utilisation, en général, d'attaques ciblées (menaces persistantes avancées).**
- **Contre le secteur public (informations politiques ou stratégiques) et le secteur privé (informations à valeur économique).**
- **Avec une énorme difficulté d'attribution.**
- **La recherche d'avantages politiques, économiques, stratégiques ou sociaux.**

La sécurité de leurs activités rend plus difficile l'analyse de ces attaques. En fait, ces dernières années, les tactiques, techniques et procédures ont fait preuve d'une professionnalisation croissante montrant clairement un nouveau type de comportement criminel, que nous pourrions appeler *Crime-as-a-Service*. Cela met à la disposition de tiers la possibilité de développer des cyberattaques à fort impact et, en général, dans le but d'obtenir des avantages économiques illicites.

Un autre élément à prendre en compte est l'utilisation du cyberespace dans ce que l'on appelle la ***guerre hybride,*** qui, en combinant différentes tactiques, cherche à déstabiliser et à polariser la société des États, en évitant les conflits armés, mais en donnant à ces actions une apparence délibérément ambiguë.

Afin de catégoriser la menace, la figure suivante montre la *pyramide des dommages*, selon le danger plus ou moins grand des cybermenaces, en fonction de leur origine.

La guerre hybride vise à déstabiliser et à polariser la société de l'UE. EÉtats.

Le niveau de danger des menaces

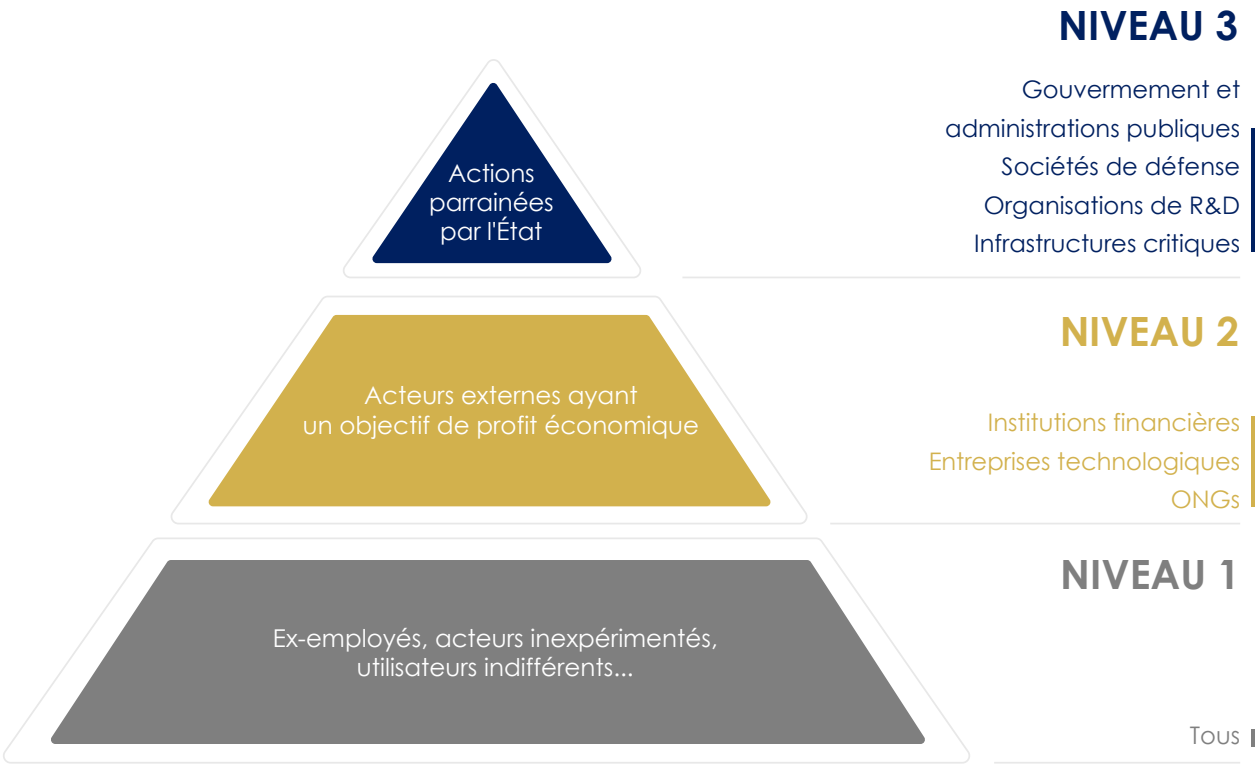


Figure 1. Pyramide des dommages

3.1 Attaques ciblées (APT)

Les cyber-attaques sont devenues une véritable alternative aux outils de renseignement conventionnels, en raison de leur faible coût, de la difficulté de prouver leur auteur et du grand volume d'informations qui peut être obtenu de cette manière.

En ce sens, les groupes APT[1] (Advanced Persistent Threat) cherchent à recueillir le plus d'informations utiles possible auprès de la victime afin de préparer l'attaque la plus efficace possible.

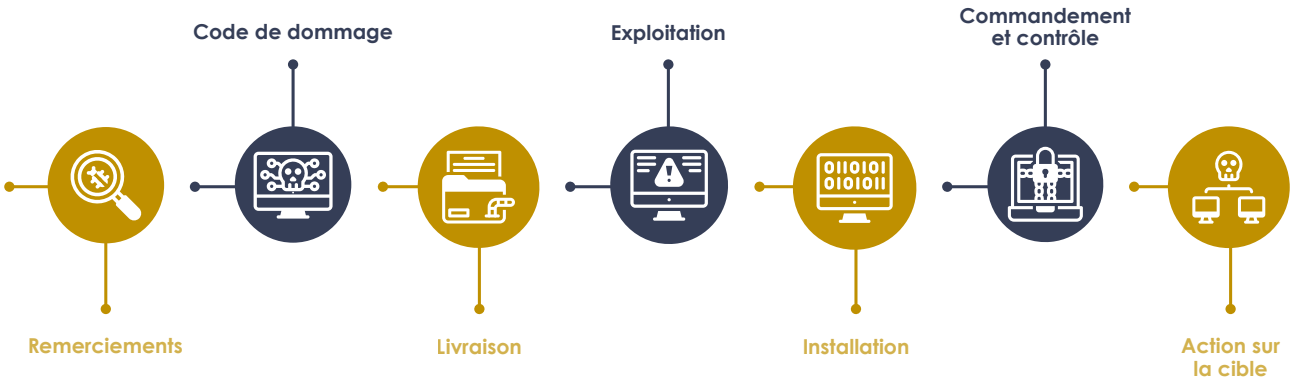


Figure 2. Phases d'un APT

1. Menaces persistantes avancées.

3. Facteurs de menace

Les paramètres qui caractérisent les techniques d'attaque (APT) sont basés sur:

Capacité de développement
Exploits[2] et vulnérabilités utilisés.

Persistance
Après les redémarrages, les mises à jour et même les activités de formatage.

Cryptage
Méthodes de cryptage et force des clés pour échanger les informations exfiltrées.

Techniques d'exfiltration
Protocoles utilisés pour l'extraction d'informations.

Cache
Rootkit[3], *bootkit* techniques utilisées pour cacher.

Résistance à l'ingénierie inverse
Techniques qui rendent l'analyse du code difficile.

Les informations exfiltrées, selon la motivation des attaquants, peuvent être de nature très variée : économiques, sensibles, propriété intellectuelle, secrets industriels ou d'Etat, etc.

2. Un programme ou un code qui exploite une vulnérabilité dans une application ou un système pour provoquer un comportement indésirable ou inattendu.
3. Un outil utilisé pour cacher une activité illégitime sur un système. Une fois installé, il permet à l'attaquant d'agir avec le niveau de privilège de l'administrateur de l'ordinateur.

4. L'internet profond

L'internet a été divisé en deux parties : le web profond et le web superficiel.

Le web superficiel est composé de pages statiques ou fixes, tandis que le web profond est composé de pages dynamiques dont le contenu est placé dans une base de données fournie à la demande de l'utilisateur.

La principale raison de l'existence de l'Internet profond est l'impossibilité pour les moteurs de recherche (Google, Yahoo !, Bing, etc.) de trouver ou d'indexer la plupart des informations qu'il contient.

Un sous-ensemble de l'internet profond n'est accessible qu'à l'aide de certains navigateurs web. C'est le cas, par exemple, du réseau TOR, où les utilisateurs doivent disposer du logiciel de navigation approprié pour accéder à des domaines inaccessibles depuis un navigateur classique.

En outre, les utilisateurs doivent connaître à l'avance l'adresse à laquelle ils doivent se rendre.

Il existe des listes avec certains domaines publics du réseau *TOR* que les utilisateurs peuvent consulter (The Hidden Wiki, Silk Road, Agora, Evolution, Middle-Earth, etc...) et des moteurs de recherche tels que "*Grams*" (le Google du *dark web*).

4.1 Le réseau TOR

The Onion Router **(TOR) est un projet conçu et mis en œuvre par la marine américaine, lancé en 2002, pour renforcer les communications sur Internet et garantir l'anonymat et la confidentialité.**

Contrairement aux navigateurs Internet classiques, TOR permet aux utilisateurs de surfer sur le web de manière anonyme. Les données ne circulent pas directement, mais passent par plusieurs nœuds qui facilitent l'anonymat des communications. Il existe un répertoire de nœuds intermédiaires avec des clés publiques associées pour établir une communication chiffrée.

TOR est chargé de créer des circuits virtuels composés de trois (3) nœuds choisis au hasard dans son réseau. Ainsi, la communication entre la source, notre ordinateur, et la destination, par exemple un site web, doit passer par les trois (3) nœuds attribués, par lesquels les informations seront transmises sous forme cryptée.

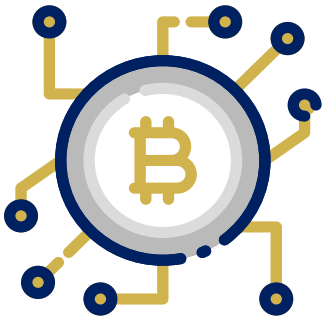
L'élément source chiffre la communication avec la clé publique du dernier nœud de la route choisie afin qu'il soit le seul élément à pouvoir déchiffrer le message et les instructions (nœuds intermédiaires et leurs clés publiques associées) pour atteindre la destination.

Des chemins aléatoires sont choisis où les données sont cryptées en couches et une fois que la dernière couche est traitée par un nœud de sortie, la connexion à la page web de destination est établie.

Contrairement aux navigateurs Internet classiques, TOR permet aux utilisateurs de surfer sur le web de manière anonyme.

4.2 Bitcoins

Elle utilise une chaîne de caractères cryptographiques qui sont échangés par le biais de portefeuilles numériques entre l'utilisateur et le vendeur, ce qui la rend hors du contrôle de tout gouvernement, institution ou entité financière.



Le *Bitcoin* est une monnaie électronique cryptée, décentralisée, d'ordinateur à ordinateur (*peer-to-peer*) où le contrôle est indirectement effectué par les utilisateurs eux-mêmes par le biais d'échanges P2P.

Au lieu de frapper une pièce de monnaie ou d'imprimer un billet, elle utilise une chaîne de caractères cryptographiques qui sont échangés par le biais de *portefeuilles* numériques entre l'utilisateur et le vendeur (échanges P2P), ce qui la rend hors du contrôle de tout gouvernement, institution ou entité financière.

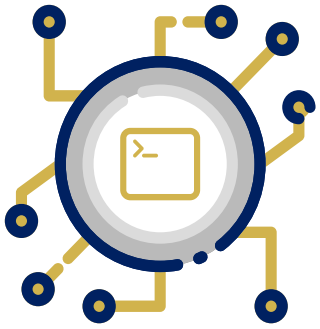
Chaque transaction avec des bitcoins est enregistrée dans une grande base de données appelée "*BlockChain*". Les données sont stockées dans des blocs et chaque nouveau bloc doit contenir le hachage du bloc précédent. Par conséquent, chaque nouveau bloc qui rejoint la chaîne possède l'historique complet de la transaction.

Ce protocole est basé sur un réseau de "mineurs" qui contrôlent la monnaie. Les mineurs mettent des ressources informatiques à la disposition du réseau et reçoivent en récompense des bitcoins. Ces mineurs protègent le système afin qu'il n'y ait pas de transactions inversées (retour de l'argent déjà dépensé).

Cette monnaie est internationale, facile à utiliser, permet des transactions anonymes, il y a des guichets automatiques et de plus en plus de vendeurs/commerçants l'acceptent. En tant que risque, il représente un mécanisme très pratique pour le blanchiment d'argent et l'évasion fiscale (exonération fiscale).

5. Applications

L'installation de logiciels peut affecter les performances et la sécurité des appareils/équipements. Il faut préserver l'intégrité des appareils/équipements et toujours installer des logiciels autorisés et fournis directement par le fabricant.



L'utilisation d'un **logiciel légitime** permet de bénéficier d'une garantie et d'une assistance, quelles que soient les implications juridiques de l'utilisation d'un logiciel non légitime.

Certification du programme pour la compatibilité avec le système d'exploitation et d'autres applications.

Installation et maintenance des **correctifs et des mises à jour de sécurité**, en accordant une attention particulière à ceux qui présentent un caractère critique.

Considérez la zone d'exposition associée **aux systèmes** (*existants*), en particulier ceux qui ont plus de dix ans en raison de leur extrême vulnérabilité.

5. Applications

Les utilisateurs doivent être **conscients** que l'introduction de logiciels non autorisés peut entraîner l'infection du système le plus protégé. Ce qui suit est indiqué comme une bonne pratique:

- **Travaillez généralement sur le système en tant qu'utilisateur non privilégié, et non en tant qu'"Administrateur".**
- **N'exécutez jamais de programmes d'origine douteuse ou inconnue.**
- **Si vous utilisez un logiciel de bureautique capable d'exécuter des macros, assurez-vous que l'exécution automatique des macros est désactivée.**

Lorsqu'il s'agit d'imprimer des documents, sachez que **les documents imprimés et les transactions sont susceptibles de faire l'objet de failles de sécurité**. Il est donc essentiel d'employer de bonnes pratiques pour se conformer à la réglementation en vigueur dans chaque entité et de veiller à ce que les informations imprimées soient sécurisées et ne soient pas accessibles par du personnel non autorisé.

> **Les introduction de logiciels non autorisés peut entraîner l'infection du système le plus.**

5.1 Cryptage des données

Le cryptage des données consiste à convertir un texte en clair en un texte illisible, appelé texte chiffré, ce qui empêche les informations d'être accessibles à des tiers non autorisés. Cela nécessite un **algorithme de cryptage** et **l'existence d'une clé**, qui permet d'effectuer le processus de transformation des données et qui doit être gardée secrète.

Il existe de nombreuses solutions commerciales[4] de cryptage des ordinateurs, qui peuvent être classées en trois (3) types selon le niveau auquel elles agissent sur le système de fichiers:

Cryptage de disque

Il s'agit d'une technologie qui crypte l'ensemble du disque, de sorte que le système d'exploitation est chargé de décrypter les informations lorsque l'utilisateur le demande.

Cryptage des dossiers

Le cryptage est effectué au niveau du dossier. Le système de cryptage crypte et décrypte les informations lorsque le dossier protégé est utilisé.

Cryptage des documents

Le système est chargé d'afficher le document et de n'en autoriser l'accès qu'aux utilisateurs autorisés, en rendant le contenu illisible aux utilisateurs non autorisés.

Le cryptage des données consiste à convertir un texte en clair en un texte illisible, appelé texte chiffré, ce qui empêche les informations d'être accessibles à des tiers non autorisés.

4. Voir le **Guide CCN-STIC-955B Recommandations d'utilisation du GPG** (https://www.ccn-cert.cni.es/series-ccn-stic/900-informes-tecnicos/1816-ccn-stic-955b-recomendaciones-de-empleo-de-gpg/file.html)

5.2 Pare-feu personnels

Les *pare-feu*[5] personnels sont des programmes qui surveillent les connexions entrantes et sortantes de votre ordinateur.

Ils sont conçus pour bloquer l'accès non autorisé à l'ordinateur, tout en permettant les communications autorisées. La partie la plus délicate d'un pare-feu est de le configurer correctement, afin de ne pas bloquer les connexions légitimes (navigation sur le Web, mises à jour, courrier électronique, etc.

En tant que critère générique, les connexions provenant de sources inconnues ne devraient pas être autorisées. Ils doivent donc bloquer toutes les connexions entrantes et n'autoriser que celles qui sont expressément indiquées sur la base d'un ensemble de règles et de critères établis.

Un pare-feu correctement configuré ajoute une protection nécessaire qui rend plus difficile les mouvements latéraux non autorisés à travers le réseau, mais ne doit en aucun cas être considéré comme suffisant.

5. Voir le **Guide CCN-STIC-408 Sécurité du périmètre - Firewall** (https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html)

5.3 Applications anti-malware

Parmi les actions qui peuvent être causées par un code malveillant ou un logiciel malveillant figurent: **la suppression ou la modification de fichiers, la consommation de ressources informatiques, l'accès non autorisé à des fichiers, l'infection à distance d'ordinateurs**, etc.

Les fonctions minimales que l'on peut attendre d'un bon **outil antimalware**[6] (plus connu sous le nom d'**antivirus**) sont le filtrage entrant et sortant des contenus malveillants, la protection dans le courrier électronique, la navigation et les connexions de toutes sortes dans les réseaux professionnels ou domestiques. Ils doivent également être capables d'analyser des fichiers sur des périphériques amovibles tels que des disques externes ou des clés USB et vous permettre de programmer des analyses complètes de temps en temps.

Les applications anti-malware doivent être régulièrement mises à jour (dernières définitions et moteurs de recherche) et être des produits de fournisseurs réputés qui permettent une combinaison des méthodes suivantes:

Scanner d'accès: permet d'examiner les fichiers lorsqu'ils sont ouverts.

Scanner à la demande: analyse basée sur un calendrier établi.

Scanner de courrier électronique: sur les appareils de protection du périmètre ou les serveurs de messagerie.

Contrôle de la signature: permet de détecter les modifications non légitimes du contenu d'un fichier.

Méthodes heuristiques: recherche d'anomalies dans les fichiers et les processus sur la base d'une expérience antérieure du comportement des logiciels malveillants.

Mais une application anti-malware seule ne suffit pas ; vous devez fournir une approche centralisée (client-serveur) pour protéger tous les terminaux (serveurs, ordinateurs de bureau, ordinateurs portables, smartphones, etc.) connectés au réseau. Certains fournisseurs proposent des systèmes de *sécurité des points finaux* qui comprennent un antivirus, un pare-feu et d'autres logiciels de sécurité.

---

6. Le CCN-CERT met à la disposition des utilisateurs enregistrés sur son portail la **plateforme multi-antivirus MARIA** pour l'analyse statique du code nuisible à travers plusieurs moteurs antivirus et antimalware pour les plateformes Windows et Linux (https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/maria-publico.html)

5.4 Effacement sécurisé des données[7]

Vous pensez peut-être que le simple fait de formater le disque dur empêchera la récupération des données qu'il contient. Cependant, il existe des applications qui permettent d'annuler le formatage d'un disque et il existe même des méthodes pour récupérer les données des disques, même s'ils ont été écrasés.

Si vous voulez vous assurer que vous ne distribuez pas d'informations sensibles, vous devez écraser les données en utilisant une méthode (modèle d'effacement) qui ne permet pas de les récupérer de quelque manière que ce soit.

Pour ce faire, il est nécessaire d'effectuer plusieurs passages en écriture sur chacun des secteurs où sont stockées les informations. Pour simplifier la tâche, le plus simple est d'utiliser une application spécialisée qui vous permet de supprimer facilement les informations.

Dans le cas des photographies numériques, des fichiers audio ou vidéo et des documents bureautiques, il existe des métadonnées qui peuvent stocker des informations cachées qui ne sont pas visibles à l'aide des paramètres standard des applications, nécessitant une configuration spécifique ou même un logiciel spécifique pour révéler ces données.

Ces métadonnées sont utiles car elles facilitent la recherche d'informations, permettent l'interopérabilité entre les organisations, fournissent une identification numérique et soutiennent la gestion du cycle de vie des documents.

Cependant, l'effacement des métadonnées ou des données cachées par le biais de procédures et d'outils de révision et de nettoyage des documents/fichiers est essentiel pour minimiser le risque que des informations sensibles soient révélées lors du stockage et de l'échange d'informations.

---

7. Voir le **Guide CCN-STIC-305 Destruction et désinfection des supports informatiques** (https://www.ccn-cert.cni.es/series-ccn-stic/300-instrucciones-tecnicas/60-ccn-stic-305-destruccion-y-sanitizacion-de-soportes-informaticos/file.html)
8. Voir le **Guide CCN-STIC-835 Effacement des métadonnées dans le cadre de l'ENS** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2031-ccn-stic-835-borrado-de-metadatos-en-el-marco-del-ens/file.html)

6. Une navigation sûre

La communication sur Internet repose sur une idée de base : des clients (ordinateurs, téléphones, tablettes, ...) appellent des serveurs (web, bases de données...) qui fournissent (servent) des informations. Cette communication s'effectue par le biais d'un protocole (http, https[9], ftp, etc.).

Le client est identifié sur le réseau par une adresse IP (TCP/IP) et chaque fois qu'il se connecte à un site web, il connaît automatiquement l'adresse IP, le nom de l'hôte, la page d'où il vient, etc. Il y a un échange d'informations qui n'est généralement pas visible, où le navigateur web est celui qui fournit la plupart de ces données.

Un pourcentage élevé d'utilisateurs n'est pas conscient de la quantité d'informations qu'ils divulguent par inadvertance et sans le vouloir à des tiers lorsqu'ils utilisent l'internet.

Un pourcentage élevé d'utilisateurs n'est pas conscient de la quantité d'informations qu'ils divulguent par inadvertance et sans le vouloir à des tiers lorsqu'ils utilisent l'internet.

Chaque fois qu'un site web est visité, des informations sont systématiquement fournies et peuvent être archivées par l'administrateur du site.

Il est trivial pour le site web de connaître l'adresse Internet de la machine à partir de laquelle vous accédez, le système d'exploitation, etc.

Grâce aux cookies, vous pouvez personnaliser davantage les informations recueillies sur les visiteurs, en enregistrant les pages les plus visitées, les préférences, l'heure de la visite, les logiciels installés, etc.

---

9. Voir le **Rapport sur les meilleures pratiques CCN-CERT BP-01/17 Recommandations pour la mise en œuvre de HTTPS** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos.html)

6. Une navigation sûre

Un navigateur web, en faveur d'une convivialité maximale, permet d'accéder à des informations apparemment inoffensives.

- L'adresse IP publique à laquelle l'utilisateur se connecte.

  Votre adresse IP est xxx.xxx.xxx.xxx.xxx.
  Votre navigateur utilise une clé secrète SSL de 128 bits.
  Le serveur utilise une clé publique SSL de 1024 bits..

- La résolution de l'écran.
- Quelles pages sont lues et celles qui ne le sont pas, quels chiffres sont regardés, combien de pages ont été visitées, quel était le site "*Referer*" le plus récemment visité.
- La valeur du champ "*User-Agent*".

  Mozilla/5.0 (Windows NT 6.1 ; rv:16.0) Gecko/20100101 Firefox/16.0

- La langue et la zone GMT du système d'exploitation.
- Accepter ou non les *cookies*.
- Polices chargées sur le système ou *plugins* installés et activés.

Voici quelques **recommandations** pour maintenir une **nnavigation sûre**[10]:

- N'accédez qu'aux sites de confiance.
- Maintenez le navigateur à jour avec la dernière version disponible auprès du fabricant.
- Configurez le niveau de sécurité du navigateur en fonction de vos préférences.
- Téléchargez des programmes à partir de sites officiels pour éviter toute usurpation d'identité malveillante.
- Configurez votre navigateur pour empêcher les fenêtres pop-up.s.
- Utilisez un utilisateur sans droits "Administrateur" pour naviguer sur Internet et empêcher l'installation de programmes et la modification des paramètres du système.

10. Voir le **Rapport sur les meilleures pratiques CCN-CERT BP-06/16 Navigation sécurisée** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1801-ccn-cert-bp-06-16-navegadores-web/file.html)

6. Une navigation sûre

- Supprimez les *cookies*, les fichiers temporaires et l'historique lorsque vous utilisez les ordinateurs d'autres personnes afin de ne laisser aucune trace de votre navigation.
- Désactivez l'option "*script*" dans les navigateurs Web, tels que Firefox (NoScript) ou Chrome (NotScript), pour empêcher l'exécution de scripts par des domaines inconnus
- Le protocole HTTPS (SSL/TLS) est recommandé par rapport au protocole HTTP, même pour les services qui ne traitent pas d'informations sensibles. Des fonctionnalités telles que HSTS et des extensions telles que *HTTPS Everywhere* contribueront à garantir que HTTPS est utilisé de préférence à HTTP lors de la navigation sur le web.
- Si possible, utilisez des machines virtuelles pour surfer sur Internet.

En outre, il faut tenir compte du fait que les systèmes de navigation anonyme permettent l'utilisation de certains services Internet, principalement ceux basés sur la navigation web (http/https), d'une manière qui n'est pas liée à l'adresse IP d'où provient la communication.

Anonymiseurs

Ils agissent comme un filtre entre le navigateur et le site web que vous voulez visiter.

Lorsque vous vous connectez à l'anonymiseur, vous entrez l'URL à visiter et ensuite il entre dans le réseau en filtrant les cookies, les javascripts, etc.

Les serveurs proxy

Un serveur proxy agit comme une passerelle entre la machine cliente et l'Internet.

Le serveur proxy agit comme un intermédiaire, il est responsable de la récupération des pages web à la place de la navigation de l'utilisateur.

Tunnels de cryptage (TOR, VPS et Darknets)

Un réseau de "tunnels" par lequel les données de navigation, dûment cryptées, passent par de multiples nœuds jusqu'à ce qu'elles atteignent leur destination.

7. Adresse email

À l'heure actuelle, le courrier électronique[11] reste l'un des outils les plus utilisés dans tout environnement d'entreprise pour l'échange d'informations, même si, ces dernières années, une multitude de technologies et d'outils collaboratifs ont vu le jour pour faciliter la communication et le partage de fichiers.

L'essor et l'efficacité de l'ingénierie sociale, qui permet de tromper les utilisateurs par le biais de courriers électroniques, ont modifié le paradigme de la sécurité des entreprises.

Actuellement, les pare-feu périmétriques et la sécurisation des services exposés à l'Internet ne sont pas des contre-mesures suffisantes pour protéger une organisation contre les attaques externes.

Quelques **recommandations**[12] pour utiliser le **courrier électronique** en toute sécurité:

- **N'ouvrez pas de lien ou ne téléchargez pas de pièce jointe à partir d'un courriel qui présente un schéma inhabituel.**
- **Ne vous fiez pas uniquement au nom de l'expéditeur. L'utilisateur doit vérifier que le domaine du courriel reçu est digne de confiance. Si un courriel provenant d'un contact connu demande des informations inhabituelles, contactez-le par téléphone ou par un autre moyen de communication pour corroborer la légitimité du courriel.**
- **Avant d'ouvrir un fichier téléchargé à partir d'un courriel, assurez-vous de son extension et ne vous fiez pas à l'icône qui lui est associée.**
- **N'activez pas les macros dans les documents Office, même si le fichier lui-même le demande.**

---

11. Voir le **Guide CCN-STIC-814 Email Security** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/524-ccn-stic-814-seguridad-en-servicio-de-correo/file.html)
12. Voir le **Rapport sur les meilleures pratiques CCN-CERT BP-02/16 E-mail** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/1598-ccn-cert-bp-02-16-correo-electronico/file.html)

7. Correo electrónico

- **Ne cliquez pas sur un lien qui vous demande des informations personnelles ou bancaires.**
- **Maintenez toujours à jour votre système d'exploitation, vos applications bureautiques et votre navigateur (y compris les *plugins*/extensions installés).**
- **Utilisez des outils de sécurité pour atténuer les exploits en plus des logiciels antivirus.**
- **Évitez de cliquer directement sur un lien à partir du client de messagerie lui-même. Si le lien est inconnu, il est conseillé de rechercher des informations à son sujet dans les moteurs de recherche tels que Google ou Bing.**
- **Utilisez des mots de passe forts pour l'accès au courrier électronique. Les mots de passe doivent être renouvelés périodiquement et, si possible, utiliser la double authentification.**
- **Cryptez les courriels contenant des informations sensibles.**

L'essor et l'efficacité de l'ingénierie sociale, qui permet de tromper les utilisateurs par le biais de courriers électroniques, ont modifié le paradigme de la sécurité des entreprises.

8. Virtualisation

La virtualisation est comprise comme la recréation d'une ressource physique (matériel) ou logique (logiciel), au moyen d'un hyperviseur qui permet son exécution par plus d'un environnement en même temps.

Dans l'environnement de la machine virtuelle, l'hyperviseur permet l'utilisation simultanée du matériel dans plus d'un système d'exploitation.

L'apogée de la virtualisation a eu lieu avec **l'utilisation du cloud**[13], où ce système de partage des ressources est devenu presque indispensable. Bien qu'il existait déjà de multiples systèmes proposés par de nombreux fabricants, leur développement et leurs progrès ont augmenté de manière exponentielle. Actuellement, vous pouvez choisir, entre autres, XenServer de Citrix, VMware ESXi de Dell, VirtualBox d'Oracle, Oracle VM Server et Hyper-V de Microsoft.

La sécurité dans la virtualisation repose sur le même principe que tout autre système, à savoir *minimiser la surface d'attaque*. Elle présente toutefois des particularités qui rendent la sécurité plus difficile, comme, par exemple, la multitude de ressources partagées ou de systèmes d'exploitation qui fonctionnent simultanément avec leurs propres applications sur la même machine physique.

13. Voir le **Guide CCN-STIC-823 Security in Cloud Environments** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html)

8. Virtualisation

En règle générale, il est **conseillé de suivre les directives suivantes lors de la** configuration d'un *hôte* de machine virtuelle:

- **Faites installer les dernières mises à jour de sécurité sur le système d'exploitation.**
- **Disposer du dernier rollback disponible du programme de virtualisation.**
- **Si possible, disposez d'au moins une carte réseau exclusivement destinée à l'infrastructure de virtualisation.**
- **Créez un environnement de laboratoire isolé de l'environnement de production.**
- **Disposez d'un groupe de sécurité pour gérer la plateforme de sécurité.**
- **Protéger les périphériques de stockage sur lesquels sont stockés les fichiers de ressources et de définition de la machine virtuelle.**
- **Gardez les administrateurs *invités* séparés des administrateurs *hôtes*.**

8. Virtualisation

Pour la création d'*invités*, il est recommandé de suivre les règles suivantes:

- **Faites un schéma préalable de ce que sera l'infrastructure de virtualisation.**
- **Dimensionnez la création de machines virtuelles en fonction des besoins réels et des ressources matérielles disponibles sur l'*hôte*.**
- **Cryptez les fichiers des machines virtuelles, les snapshots et les disques durs virtuels pour le stockage des plateformes de virtualisation.**
- **Installez les dernières mises à jour de sécurité sur chaque système d'exploitation *invité*.**
- **Évaluez l'installation des agents de l'hyperviseur, type Guest Additions, et dans le cas où vous le faites, tenez-les à jour.**
- **Sécurisez tous les systèmes d'exploitation invités à l'aide de logiciels anti-malware et de pare-feu.**
- **Ne branchez les DVD, les CD et les supports de stockage externes que lorsque cela est nécessaire et éteignez-les après utilisation.**
- **Ne gardez actives que les machines virtuelles essentielles.**
- **Utilisez une interface réseau virtuelle distincte pour la connexion au réseau de l'entreprise ou à Internet, qui doit être désactivée lorsqu'elle n'est pas utilisée.**
- **Cryptez les supports de stockage externes contenant les fichiers de virtualisation de sauvegarde et sécurisez-les de manière appropriée.**

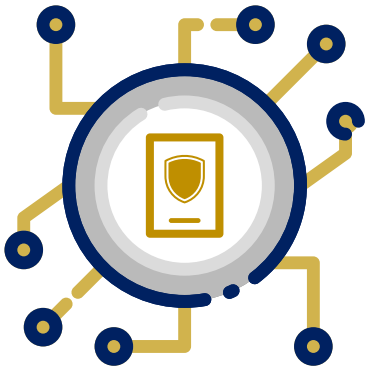
9. Sécurité des appareils mobiles

L'augmentation des possibilités et des capacités associées aux appareils mobiles[14] de nos jours implique également des risques accrus pour leur sécurité.

Il est très important que les utilisateurs soient conscients de l'importance de la sécurité des appareils mobiles et des dangers qui peuvent résulter de leur mauvaise utilisation.

Il est conseillé de suivre ces **conseils**[15] :

L'augmentation des possibilités et des capacités associées aux appareils mobiles[14] de nos jours implique également des risques accrus pour leur sécurité.



- **Mettez en place une méthode sécurisée pour déverrouiller le terminal, par exemple en utilisant une *phrase de passe* forte.**
- **Il est conseillé de supprimer les aperçus des messages et de prendre des précautions supplémentaires lorsque le téléphone n'est pas à portée de main.**
- **Désactivez les connexions sans fil (WiFi, Bluetooth, etc.) et toutes les connexions inutiles lorsque vous ne les utilisez pas.**

14. Voir les différents **Guides CCN-STIC 450-451-452-453-454 et 455 Security on Mobile Devices** (https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/6-ccn-stic-450-seguridad-en-dispositivos-moviles/file.html)
15. Voir le **Rapport sur les meilleures pratiques CCN-CERT BP-03/16 Appareils mobiles** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1807-ccn-cert-bp-03-16-dispositivos-moviles-1/file.html)

9. Sécurité des appareils mobiles

- **Maintenez le logiciel de l'appareil à jour et utilisez une configuration de sécurité approuvée par le responsable TIC de l'entité.**
- **Faites attention aux demandes d'accès et de permission des applications exécutées sur votre téléphone.**
- **Ignorez et supprimez les messages (SMS, MMS ou autres) de sources inconnues qui vous invitent à télécharger du contenu ou à accéder à des sites web.**
- **Activez l'accès par code PIN aux connexions Bluetooth et mettez l'appareil en mode furtif. N'acceptez pas les connexions provenant de dispositifs inconnus.**
- **Téléchargez des applications uniquement à partir des magasins officiels. Ne téléchargez en aucun cas des logiciels à partir de sites non fiables et demandez en tout cas au responsable TIC de l'entité les applications nécessaires.**
- **Évitez de *jailbreaker* ou de *rooter* le combiné, car cela peut compromettre et réduire considérablement la sécurité du téléphone, même s'il est tentant d'accéder à des applications ou des services spécifiques.**
- **Utilisez un réseau privé virtuel (VPN[16]) pour protéger le trafic de données entre le dispositif mobile et l'infrastructure de l'entité. C'est toujours une bonne pratique d'éviter une éventuelle surveillance par des intrus.**
- **Évitez autant que possible l'utilisation d'imprimantes, de télécopieurs ou de réseaux WiFi publics, tels que ceux proposés dans les hôtels ou les aéroports, à moins que vous ne disposiez des outils nécessaires pour sécuriser vos communications.**
- **De nombreux téléphones mobiles et appareils photo numériques ajoutent les coordonnées GPS dans les informations des images prises, il est donc conseillé de limiter le partage des images sur le réseau ou d'utiliser des applications qui suppriment ces informations.**
- **Séparer les communications personnelles et professionnelles est une bonne pratique de sécurité. Le fait d'avoir des compartiments étanches dans un seul appareil augmentera la sécurité.**
- **Mettre en œuvre une gestion centralisée des appareils mobiles à l'aide d'agents *MDM* (Mobile Device Management).**
- **Pour traiter des informations sensibles, n'utilisez que des solutions approuvées par le responsable de la sécurité des TIC de l'entité.**

---

16. Voir le **Guide CCN-STIC-836 Sécurité des réseaux privés virtuels (VPN)** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2299-ccn-stic-836-seguridad-en-vpn-en-el-marco-del-ens/file.html)

10. Sécurité des réseaux sans fil

Si vous travaillez avec un réseau sans fil, pour maximiser la sécurité du réseau WiFi, il est nécessaire de prêter attention aux **recommandations**[17] suivantes:

Modifiez le mot de passe de connexion par défaut pour l'administration du point d'accès.

Modifier le SSID configuré par défaut en n'utilisant pas de noms qui pourraient identifier l'entité et lui permettre de passer inaperçue dans l'environnement.

En masquant l'identifiant SSID de l'extérieur, il est difficile d'obtenir le nom du réseau, bien que la traçabilité du client soit toujours possible, indépendamment du masquage du SSID.

Activez le filtrage des adresses MAC des appareils WiFi pour permettre aux appareils ayant les adresses MAC spécifiées de se connecter au réseau.

Configurez WPA2-AES en mode confidentialité des données, pour obtenir une authentification forte et un chiffrement des données.

17. Voir le **Guide CCN-STIC-816 Sécurité dans les réseaux sans fil** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2317-ccn-stic-816-seguridad-en-redes-inalambricas-en-el-ens/file.html)

Limitez la couverture du réseau local sans fil. Une antenne multidirectionnelle située au centre de la maison ou du bureau est le choix le plus courant.

Déconnectez le réseau lorsqu'il n'est pas utilisé. Bien qu'il ne soit pas pratique de le faire quotidiennement, il est fortement recommandé de le faire pendant les longues périodes d'inactivité.

Désactivez UPnP (Universal Plug and Play) lorsque son utilisation n'est pas nécessaire, afin d'éviter que des codes malveillants provenant du réseau lui-même ne l'utilisent pour franchir le pare-feu du routeur et permettre à d'autres attaquants d'y accéder.

Mettez périodiquement à jour le *micrologiciel du* routeur, car un grand nombre de mises à jour et de correctifs ajoutés ont une incidence sur la sécurité.

Utilisez des adresses IP statiques ou limitez le nombre d'adresses réservées (DHCP) lorsque cela est possible, pour empêcher les utilisateurs non autorisés d'obtenir une adresse IP à partir du réseau local.

Activez le pare-feu du routeur, afin que seuls les utilisateurs et les services autorisés puissent accéder au réseau.

Activez l'option de *connexion* pour le routeur et analysez périodiquement l'historique des accès.

Il est conseillé de changer le DNS par défaut configuré par le routeur pour un autre qui préserve la confidentialité de l'utilisateur et améliore sa sécurité, par exemple, *DNSCrypt*.

11. Messagerie instantanée

Les applications de messagerie instantanée vous permettent d'envoyer des messages texte via une connexion Internet (WhatsApp[18] et Telegram[19] sont les plus connues).

Dans le cas de WhatsApp, lancé en 2009, par exemple, il traite actuellement environ 100 milliards de messages par jour.

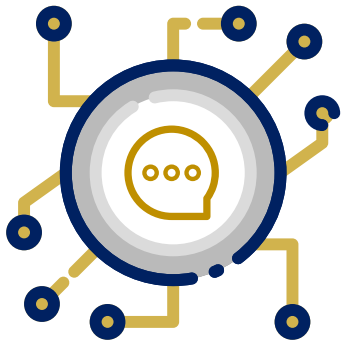
Il s'agit de plateformes qui peuvent se comporter de manière similaire à un réseau social classique et qui sont susceptibles de s'étendre. En outre, le partage d'informations personnelles et la faible perception du risque que les utilisateurs ont en matière de sécurité en ont fait un environnement attrayant pour les intrus et les cyberattaquants qui tentent d'obtenir des données et des informations de leurs utilisateurs.

L'un des défauts les plus courants des applications de messagerie est la manière dont elles suppriment les conversations stockées sur le téléphone. En effet, il ne s'agit pas d'une suppression directe des messages, mais ceux-ci sont marqués comme libres, de sorte qu'ils peuvent être écrasés par de nouvelles conversations ou données en cas de besoin et être accessibles par des techniques de police scientifique.

Soyez également conscient des implications lorsque vous avez l'option de sauvegarde active (stockage d'une éventuelle conversation supprimée) qui pourrait être récupérée à l'avenir.

Lors de l'établissement de la connexion avec les serveurs, des informations sensibles sur l'utilisateur peuvent être échangées en clair et exposées à n'importe qui lors de l'utilisation de réseaux WiFi publics ou d'origine douteuse.

Le partage des informations personnelles et la faible perception des risques par les utilisateurs ont fait des applications de messagerie instantanée applications de messagerie instantanée un environnement attrayant pour cyberattaquants.



18. Voir **CCN-CERT IA-21/16 Risques liés à l'utilisation de WhatsApp** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1746-ccn-cert-ia-21-16-riesgos-de-uso-de-whatsapp/file.html)
19. Voir **CCN-CERT IA-23/17 Risques d'utilisation de Telegram** (https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2443-ccn-cert-ia-23-17-riesgos-de-uso-de-telegram-1/file.html)

11. Messagerie instantanée

Système d'exploitation du client

Version de l'application utilisée

Numéro de téléphone enregistré

En utilisant une connexion VPN, toutes les données envoyées et reçues sont cryptées entre l'expéditeur et le destinataire, ce qui ajoute une nouvelle couche de sécurité pour empêcher les attaquants d'intercepter le trafic réseau (*man-in-the-middle*).

En revanche, la base de données des conversations, des fichiers, des messages, ainsi que d'autres données traitées par ce type d'application est stockée localement sur le téléphone, que l'option "*sauvegarde*" dans le nuage soit activée ou non sur l'appareil.

Bien que les informations soient stockées cryptées localement, il existe une multitude d'applications[20] qui, par exemple pour *WhatsApp,* permettent de décrypter simplement les informations contenues, aussi bien en version locale pour un ordinateur, qu'à travers une application sur le téléphone ou une interface web.

Pour empêcher un pirate d'accéder à toutes les informations privées stockées sur votre téléphone, vous devez prêter une attention particulière aux applications tierces qui sont installées, ainsi qu'à l'accès physique d'une autre personne au combiné.

Dans le cas du partage de données avec des réseaux sociaux, tels que *WhatsApp* et *Facebook*, et bien que les messages, les photos et les informations de profil ne soient pas ciblés pour le partage, d'autres informations telles que le numéro de téléphone, les contacts, la dernière heure de connexion, ainsi que vos habitudes d'utilisation des applications, peuvent être partagées.

20. WhatCrypt: http://whatcrypt.com/

11. Messagerie instantanée

En insistant sur les **recommandations** indiquées pour les appareils mobiles, il sera nécessaire de prendre certaines précautions dans l'utilisation des applications de messagerie instantanée telles que:

- **Gardez votre téléphone verrouillé. Cela permettra de réduire le risque si l'appareil tombe entre de mauvaises mains.**
- **Il serait souhaitable de supprimer les aperçus des messages et de prendre des précautions supplémentaires lorsque le téléphone n'est pas à portée de main.**
- **Dans la mesure du possible, il est recommandé de configurer les applications de manière à ce qu'elles ne reçoivent des messages que des personnes autorisées.**
- **Désactivez toute connectivité supplémentaire sur le téléphone lorsqu'il n'est pas utilisé, comme le WiFi ou le Bluetooth, car cela permet non seulement de réduire la consommation de la batterie, mais aussi de réduire la surface d'attaque potentielle sur l'appareil.**
- **Utilisez des applications de messagerie instantanée dont le code source est ouvert à la communauté et a été examiné. Dans ce sens, il existe des alternatives qui assurent également la confidentialité des communications, en chiffrant le trafic de bout en bout (e2e), un exemple est *Signal*.**

12. Les réseaux sociaux

Les médias sociaux ont non seulement changé la façon dont les citoyens s'informent et communiquent entre eux, mais aussi la façon dont les gouvernements et les organisations transmettent leurs messages aux citoyens et la façon dont ceux-ci réagissent.

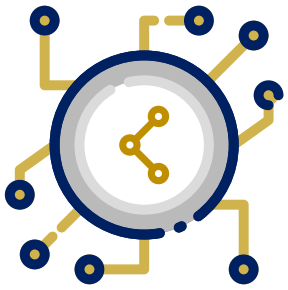
Communiquer, partager des informations, maintenir le contact par intérêt ou affinité, entrer en relation, se forger une identité et une réputation, revendiquer, protester, manipuler... les objectifs recherchés lors de l'utilisation de tel ou tel réseau social sont multiples.

Cependant, le succès rencontré, les énormes possibilités qu'ils offrent et leur utilisation massive les ont placés dans la ligne de mire des cyberattaquants, qui n'hésitent pas à exploiter les risques et les vulnérabilités que présentent à la fois les plateformes qui supportent ces réseaux sociaux et les personnes ou organisations qui les utilisent.

Une fois de plus, le maillon faible de cette chaîne est le facteur humain en raison d'un manque de sensibilisation et d'une confiance excessive dans l'utilisation de ces réseaux.

En général, les risques associés aux réseaux sociaux sont les mêmes que ceux d'autres activités et/ou services sur Internet : grande difficulté à supprimer les informations téléchargées, accès futur par des tiers (le droit de changer d'avis est nul et il sera très difficile de supprimer toute opinion, photographie ou vidéo téléchargée sur le réseau) et difficulté de discerner entre une information véridique et une propagande ou une manipulation.

À ce stade, il faut rappeler l'importance des paramètres de sécurité de l'appareil (système d'exploitation et navigateur) utilisé pour se connecter à Internet et donc accéder aux réseaux sociaux.



Cependant, le succès rencontré, les énormes possibilités qu'ils offrent et leur utilisation massive les ont placés dans la ligne de mire des cyberattaquants.

12. Les réseaux sociaux

Voici les **principaux conseils que l'on** peut donner comme bonnes pratiques dans l'utilisation des **réseaux sociaux**:

- **Création minutieuse du profil et des paramètres de confidentialité. Ne vous fiez pas aux paramètres par défaut fournis par les plateformes.**
- **Réfléchissez à tout ce que vous publiez et utilisez un pseudonyme. Supposer que tout ce que vous publiez sur un réseau social est permanent, même si vous supprimez votre compte.**
- **Choisir nos amis avec soin.**
- **Pour éviter de révéler les adresses électroniques de vos amis, n'autorisez pas les services de réseaux sociaux à analyser votre carnet d'adresses électroniques.**
- **Faites attention aux services de géolocalisation et aux informations sur les téléphones portables.**
- **Attention aux liens. Évitez de cliquer sur des hyperliens ou des liens d'origine douteuse.**
- **Saisissez l'adresse de votre site de réseau social directement dans votre navigateur pour éviter qu'un faux site ne vole vos informations personnelles.**
- **Soyez prudent lorsque vous installez des éléments supplémentaires sur votre site, car ces applications sont parfois utilisées pour voler des informations personnelles.**
- **Examinez les informations que vous publiez. Évitez de donner trop d'informations sur vous-même, comme votre date d'anniversaire, votre ville natale, votre classe de lycée, etc. afin d'empêcher les gens de pirater votre compte.**
- **Sécurité des mots de passe, utilisez des mots de passe complexes comprenant des chiffres, des symboles et des signes de ponctuation. Il est important de ne pas partager le même mot de passe pour tous les réseaux sociaux et autres services utilisés sur Internet (utilisez des gestionnaires de mots de passe tels que *keepass*).**
- **Renforcer la sécurité de l'accès au compte en ajoutant une authentification par second facteur (2FA) qui empêche un attaquant potentiel ayant obtenu le mot de passe d'accéder au service.**

13. L'internet des objets (IoT)

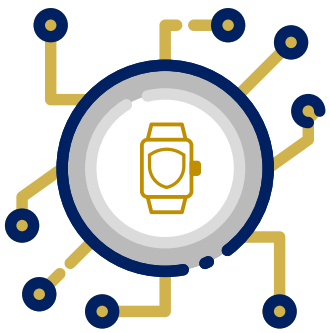
En substance, l'IoT[21] (*Internet of Things*) désigne des réseaux d'objets physiques, d'artefacts, de véhicules, de bâtiments, d'appareils, de vêtements, d'implants, etc. qui portent en eux des composants électroniques, des logiciels, des capteurs avec une connectivité réseau qui leur permet de collecter des informations pour parvenir à une contextualisation de la situation grâce à des techniques de Big Data impossibles à réaliser par d'autres moyens.

Il s'agit d'un réseau qui interconnecte des milliers d'objets physiques offrant des données en temps réel, devenant ainsi les capteurs du monde physique. À ce stade, nous devons prendre en considération le changement culturel qu'ils impliquent, car la technologie influence la façon dont nous prenons des décisions et cela affecte la capacité d'action, la vie privée et l'autonomie des personnes.

L'IdO est la première véritable évolution de l'internet, un saut qui pourrait déboucher sur des applications révolutionnaires capables de changer radicalement notre façon de vivre, d'apprendre, de travailler, de nous divertir ou d'interagir socialement.

Les objets du quotidien ne sont plus des objets isolés, mais des appareils qui peuvent à leur tour être connectés à d'autres appareils. Le cauchemar des experts en cybersécurité peut devenir des armées de "*botnets*" utilisant des grille-pain intelligents pour développer des attaques DDoS ou pour cacher des informations et des exécutables à l'abri des regards des chercheurs.

L'IdO est la première véritable évolution de l'internet, un saut qui pourrait déboucher sur des applications révolutionnaires capables de changer radicalement notre façon de vivre, d'apprendre, de travailler, de nous divertir ou d'interagir socialement.



21. Voir le **Rapport sur les meilleures pratiques CCN-CERT BP-05/16 Internet des objets** (https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2258-ccn-cert-bp-05-16-internet-de-las-cosas/file.html)

13. L'internet des objets (IoT)

Dans l'IdO, il est nécessaire de prendre en compte des **aspects d'une importance vitale** tels que la sécurité, l'interopérabilité et la gérabilité de ces systèmes:

Interface web.

Mécanismes d'authentification.

Services de réseau.

Transport non crypté.

Protection de la vie privée.

Paramètres de sécurité.

Intégrité du logiciel/firmware.

Sécurité physique des dispositifs.

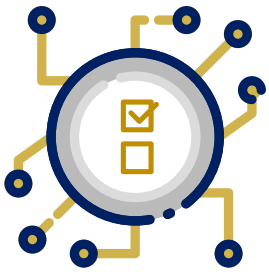
13. L'internet des objets (IoT)

Le défi revient à établir une base de surveillance et de contrôle pour réduire l'exposition aux risques et appliquer des techniques intelligentes à la population croissante d'appareils IoT.

- **Changez les mots de passe par défaut sur les appareils et utilisez des mots de passe vraiment forts.**
- **Maintenez les appareils à jour avec les dernières versions de logiciels et de micrologiciels disponibles.**
- **Désactivez toutes les connexions à distance (internet) des appareils lorsqu'elles ne sont pas strictement nécessaires.**
- **Ne gardez ouverts que les ports de communication réellement nécessaires et modifiez les ports d'écoute si possible.**
- **Si les dispositifs IoT ne permettent pas de configurer leur sécurité, faites-les toujours fonctionner sur un réseau local (LAN) derrière un dispositif (routeur) correctement configuré qui assure cette sécurité.**
- **Dans la mesure du possible, assurez l'authenticité, la confidentialité et l'intégrité de toutes les communications locales (LAN), surtout si elles sont effectuées par des liaisons radio (WiFi, Bluetooth, etc.).**
- **Vérifier périodiquement la configuration de la sécurité de tous les éléments de l'architecture IoT et de sa communication avec l'extérieur.**
- **Maintenir désactivés les composants inutiles, tels que les microphones, les caméras vidéo, etc., selon le cas...**
- **Vérifiez la visibilité de vos propres dispositifs dans les moteurs de recherche de dispositifs IoT tels que Shodan.**

14. Politique de sécurité

La conception d'une stratégie de sécurité au sein d'une organisation dépend généralement de son activité, de sa taille, de son champ d'action et de son interconnexion avec les utilisateurs externes (clients, fournisseurs, utilisateurs finaux, etc.). Toutefois, d'une manière générale, certaines étapes de basepeuvent être envisagées lors de l'élaboration d'une stratégie:



Créer une politique de sécurité.

Effectuer une analyse des risques.

Mettre en œuvre des mesures de protection appropriées.

Sensibiliser les utilisateurs.

La **politique de sécurité**[22] établit l'état des informations et des services au sein de l'entité et définit ce qui doit être protégé, ainsi que les objectifs de sécurité correspondants, fournissant ainsi une base pour la planification de la sécurité.

Il décrit les responsabilités des utilisateurs et la manière dont l'efficacité des mesures appliquées est contrôlée. En bref, il s'agit d'un ensemble de règles que vous décidez d'appliquer aux activités du système et aux ressources de communication appartenant à une organisation.

22. Voir **CCN-STIC-805 Politique de sécurité de l'information** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/508-ccn-stic-805-politica-de-seguridad-de-la-informacion/file.html)

14. Politique de sécurité

Ces règles portent sur des domaines tels que la sécurité physique, la sécurité du personnel, la sécurité administrative et la sécurité du réseau. En outre, elle doit indiquer l'importance des technologies de l'information pour l'organisation, la période de validité de la politique, les ressources disponibles et les objectifs spécifiques à couvrir.

L'**analyse des risques**[23] identifie les risques auxquels l'organisation est exposée et quels sont les impacts, les menaces potentielles et les vulnérabilités qui peuvent être exploitées par ces derniers.

Une fois la politique de sécurité établie, en déterminant le risque résiduel que vous êtes prêt à accepter, vous devez établir les **mesures de protection** qui s'y conforment.

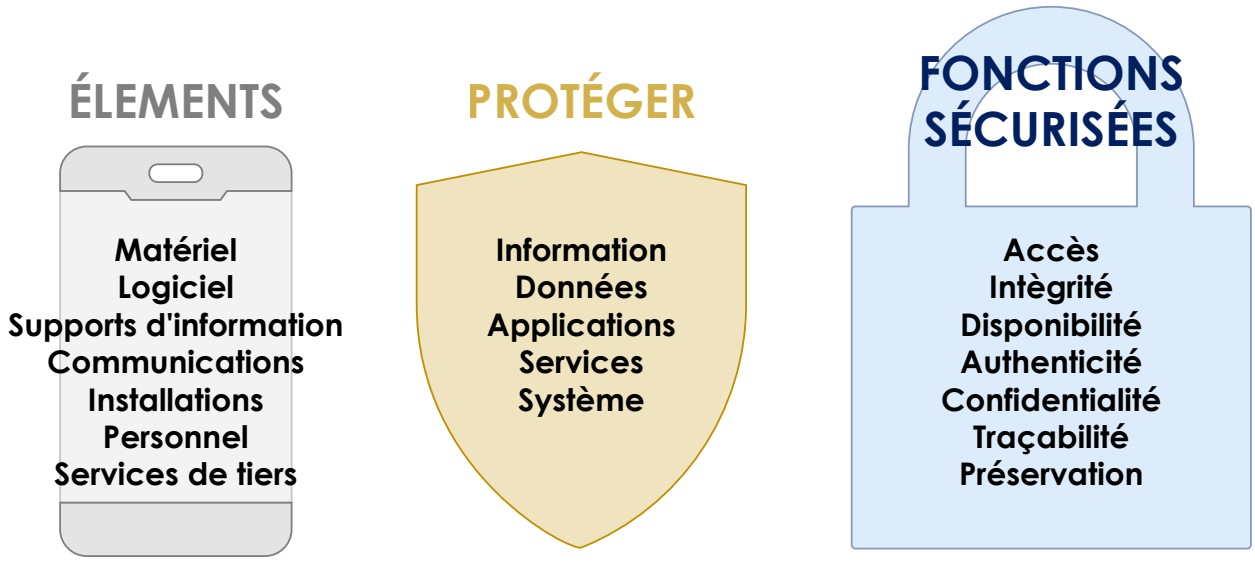


Figure 3. Éléments à prendre en compte dans la politique de sécurité

23. CCN-CERT met l'outil d'**analyse de risque PILAR** à la disposition du secteur public (https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar.html)

14. Politique de sécurité

La gestion des risques utilise les résultats de l'analyse des risques pour sélectionner et mettre en œuvre des **mesures de sécurité** appropriées afin de contrôler les risques identifiés, qui peuvent être divisés comme suit:

- **Préventives: elles visent à réduire le risque.**
  - **Protection Physique**: gardiennage, contrôle d'accès, protection matérielle...
  - **Mesures Techniques**: pare-feu, détecteurs d'intrusion, cryptographie...
  - **Mesures Procédurales**: cours de sensibilisation, cours de recyclage, règles d'accès à l'information, sanctions, etc.
- **Analyse: vise à identifier le risque.**
  - **Protection Physique**: systèmes de surveillance, détecteurs de mouvement...
  - **Mesures Techniques**: contrôle d'accès logique, session d'authentification...
  - **Mesures procédurales**: gestion des journaux, suivi des audits...
- **Correctif: vise à prévenir ou à réduire l'impact sur les actifs.**
  - **Protection Physique**: alimentation de secours (UPS)...
  - **Mesures Techniques**: programme antivirus, audits, sauvegarde de sécurité...
  - **Mesures procédurales**: plans d'urgence...

14. Politique de sécurité

Les personnes constituent la menace la plus sérieuse pour un système d'information. Leur **formation et leur sensibilisation** sont donc l'un des objectifs fondamentaux à poursuivre avec la mise en œuvre d'un programme de culture de la cybersécurité.

Le programme de sensibilisation doit faire comprendre non seulement comment protéger les systèmes, mais aussi pourquoi il est important de les protéger et comment les utilisateurs deviennent la première barrière de sécurité pour ces systèmes.

Enfin, il est très important de définir, documenter et diffuser une politique de sécurité qui démontre l'engagement de l'organisation en matière de sécurité, ainsi que l'élaboration d'une réglementation qui fixe les obligations auxquelles sont soumis les utilisateurs en matière de traitement et de sécurité des informations.

Personnes constituent la menace la plus sérieuse pour un système d'information. Leur formation et leur sensibilisation sont donc l'un des objectifs fondamentaux.

14.1. Gouvernance

Les professionnels sont la base d'une opération de sécurité réussie. C'est pourquoi des aspects tels que la gouvernance, la structure, l'expérience, la formation et la certification du personnel doivent être pris en compte dans toute organisation.

Des mécanismes de **gestion** et d'**administration de la sécurité** doivent être établis, y compris le soutien aux opérations, les niveaux d'escalade en fonction de la classification et de la remédiation des incidents, la fréquence et les types de notification, etc. En ce sens, il est conseillé de mettre en œuvre ce que l'on appelle le **SMSI (système de gestion de la sécurité de l'information),** un ensemble de politiques de gestion de l'information, où un ensemble de processus sont définis, mis en œuvre et maintenus pour gérer efficacement l'accessibilité de l'information, en cherchant à assurer la confidentialité, l'intégrité et la disponibilité des actifs informationnels tout en minimisant les risques de sécurité de l'information.

Ainsi, la **structure** doit permettre d'identifier les personnes qui ont le niveau d'autorité et de responsabilité pour les différentes tâches.

Les domaines d'expertise nécessaires sont ceux qui permettront de définir les rôles et les profils nécessaires au fonctionnement des services, étant important de considérer les plans de formation et les certifications qui donnent lieu à l'adaptation aux changements, à l'incorporation de nouvelles technologies et à la croissance des services.

14. Politique de sécurité

Il convient d'envisager la création d'un bureau de sécurité chargé d'aider à la mise en œuvre des politiques, procédures et réglementations qui jettent les bases de la direction, de la gestion, de la communication, de l'évaluation, du contrôle et de l'amélioration de la sécurité des informations liées aux activités propres de l'entité, conformément aux réglementations et bonnes pratiques applicables:

- **Examiner et soutenir la mise en œuvre du modèle de gouvernance.**
- **Analyse et adaptation de la réglementation.**
- **Analyse et gestion des risques associés aux actifs (risque résiduel assumable).**
- **Analyse et définition des tableaux de bord (mesures et indicateurs).**
- **Audits de conformité réglementaire.**
- **Soutien aux organes directeurs de la sécurité.**
- **Suivi et amélioration du statut et de la gestion de la sécurité.**

14.2 Gestion de la configuration

La mise en œuvre efficace du contrôle de la **configuration et de la gestion des logiciels** est essentielle, car c'est le seul moyen de garantir que les systèmes d'exploitation et les applications sont correctement mis à jour après la publication des correctifs nécessaires.

Les éléments suivants doivent être pris en compte:

La sécurité offerte par les mots de passe dépend, dans une large mesure, de leur confidentialité.

Tous les fichiers exécutables partagés et les *modèles* de documents doivent être placés dans un répertoire en lecture seule.

Chaque utilisateur doit disposer de son propre répertoire personnel sur le réseau avec un accès en lecture/écriture et un accès en lecture restreint pour les autres utilisateurs afin d'éviter la propagation prévisible de logiciels malveillants de la machine locale vers le réseau.

Les répertoires partagés par plusieurs utilisateurs sont une façon courante de travailler, il est donc nécessaire d'empêcher la propagation d'éventuelles infections.

Les **mots de passe** sont le principal mécanisme d'authentification utilisé par les personnes pour accéder aux systèmes d'information. La sécurité offerte par les mots de passe dépend, dans une large mesure, de leur confidentialité.

- **Il ne peut être facilement associé à aucune information relative à l'utilisateur du compte.**
- **Il aura une longueur minimale de huit (8) caractères avec différents types de caractères typographiques.**
- **Changez régulièrement votre mot de passe.**
- **Ne partagez pas les comptes et les mots de passe avec d'autres utilisateurs.**
- **Ne notez pas les mots de passe dans des endroits facilement accessibles et ne les stockez pas dans des fichiers non protégés sur votre ordinateur.**
- **Limiter la possibilité de "*Se souvenir du mot de passe*" offerte par certains navigateurs web.**

Il existe des programmes qui vous permettent de stocker tous les mots de passe avec les noms d'utilisateur associés en un seul endroit, afin qu'ils soient toujours disponibles et que vous n'ayez pas besoin de tous les retenir. En général, ces programmes disposent également d'un générateur de mots de passe, afin de pouvoir les générer en toute sécurité.

Les **upports amovibles** constituent l'une des plus grandes menaces de fuite de données et d'infection par des logiciels malveillants. Limiter l'utilisation des dispositifs USB est peut-être trop radical. Cependant, vous devriez envisager de bloquer ces ports et de retirer les lecteurs/graveurs de supports optiques des ordinateurs des utilisateurs.

14.3 Surveillance

Parallèlement au contrôle de la configuration et à la gestion des logiciels, un processus continu d'analyse des vulnérabilités doit être évalué, de manière automatique ou manuelle.

Analyse automatique de la vulnérabilité:
déploiement d'outils permettant d'effectuer des analyses de la vulnérabilité des infrastructures et des services.

Analyse manuelle des vulnérabilités:
un groupe d'analystes effectue un examen périodique des différentes applications, principalement celles exposées à l'Internet, du point de vue de la boîte noire et de la boîte blanche.

Centre des Opérations de Cybersécurité (SOC)

DÉTECTION

Système d'alerte précoce

ANALYSE

Analyse des codes nuisibles

RÉPONSE

Gestion des incidents

COORDINATION

Informations sur les cybermenaces

Il ne faut pas perdre de vue qu'en mettant en place un **Centre d'Opérations de Sécurité (SOC)**, les capacités de surveillance et de détection des incidents sont améliorées et la capacité à réagir et à répondre à toute attaque est optimisée.

Envisagez le déploiement d'un bloc de services basé sur:

Surveillance de la sécurité

Déploiement de sondes à haute capacité qui reçoivent une copie du trafic Internet entrant et sortant. Traitement des événements générés par un système de gestion des informations et des événements de sécurité (SIEM).

Des modules de *Machine Learning* sont également à envisager pour l'analyse des événements et des alertes et pour pouvoir détecter de nouvelles menaces.

Protection et filtrage des contenus malveillants

Protégez les utilisateurs qui surfent sur Internet contre ce type de menace. Les dispositifs de nouvelle génération, qui disposent, en plus des capacités traditionnelles des pare-feu, de la prévention des intrusions et du contrôle des applications.

Réponse aux incidents

Service avancé de soutien à la gestion des incidents par le biais de professionnels capables de coordonner, à distance ou sur place, avec le personnel de l'entité afin d'effectuer une analyse médico-légale, de collaborer à la stratégie d'atténuation et/ou de récupération, etc.

Analyse des vulnérabilités

Analyse périodique des vulnérabilités, à la fois automatisée et manuelle. À cette fin, des technologies de balayage des systèmes et des applications web seront fournies pour faciliter l'exécution de ces tests périodiques, tant automatisés que manuels.

Le constitution de a SOC permet à amélioration des capacités de détection et de surveillance des incidents, ainsi que ainsi que optimiser la capacité de réagir et de répondre à toute attaque.

14.4 Politiques de continuité des affaires et de sauvegarde

Le terme "*continuité des activités*" implique de réfléchir et de disposer d'un plan alternatif au cas où un désastre se produirait dans les systèmes TIC de l'entité. Ce plan doit être documenté afin que, en cas de catastrophe, les étapes à suivre pour atténuer le problème et revenir le plus rapidement possible à la situation antérieure de normalité soient claires.

En outre, dans la mesure du possible, les plans de continuité doivent être **testés pour confirmer** qu'ils sont à jour et répondent efficacement au besoin.

Des **sauvegardes régulières** sont essentielles pour garantir l'intégrité/disponibilité du système. La sauvegarde consiste à créer une copie des données sur un support différent de celui où elles se trouvent afin de pouvoir restaurer la copie originale après une perte de données.

La perte de données peut être due à un vol, à une panne de système, à une catastrophe naturelle ou simplement à une défaillance matérielle du système. Il existe de nombreux types de dispositifs de stockage de données utilisés pour les *sauvegardes*, avec des avantages et des inconvénients à prendre en compte lors de leur choix.

Enfin, il est fortement recommandé de vérifier les sauvegardes relativement fréquemment en restaurant réellement les données sur un emplacement de test.

14.5 Gestion des incidents

La gestion des incidents[24] fait partie de la culture de gestion des risques.

Lorsqu'un incident de[25] sécurité se produit, il est essentiel pour une organisation de disposer d'un protocole d'intervention efficace pour aider les équipes de sécurité à minimiser la perte ou la fuite d'informations, à empêcher la propagation de l'incident, voire l'interruption du service lui-même. La rapidité avec laquelle l'incident est reconnu, analysé et traité permet de limiter les dégâts et de minimiser le coût de la récupération.

Les organisations doivent s'habituer à signaler et à partager les incidents avec les organisations concernées, d'autant plus que les schémas se répètent souvent. Il est essentiel d'établir de bonnes pratiques en matière de notification, d'utilisation d'une taxonomie commune et de procédures de notification des incidents, y compris ceux dont l'impact est inconnu.

Les organisations doivent s'habituer à signaler et à partager les incidents avec les organisations concernées, d'autant plus que les schémas se répètent souvent.

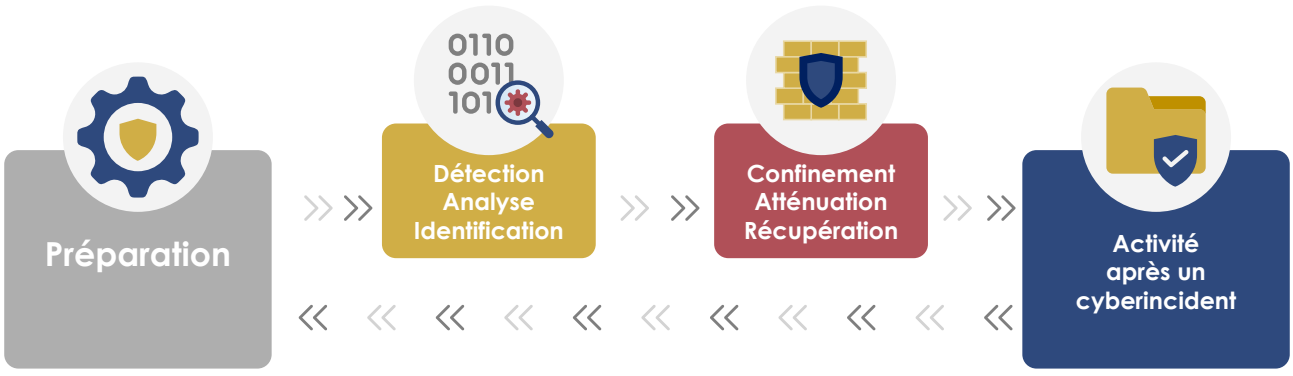


Figure 4. Cycle de vie de la réponse aux cyberincidents

24. Voir le **Guide CCN-STIC-817 Gestion des incidents** (https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html)
25. Événement inattendu ou indésirable ayant des conséquences préjudiciables à la sécurité des réseaux et des systèmes d'information

À cet égard, les autorités compétentes et les CERT/CSIRT[26] de référence utilisent une plateforme commune pour faciliter et automatiser les processus de notification, de communication et de signalement des incidents.

Les entités concernées procèdent sans délai à une première notification. Par la suite, ils effectuent les notifications nécessaires pour mettre à jour les informations sur l'évolution de l'incident jusqu'à sa résolution. Une fois l'incident résolu (les réseaux et les systèmes ont été restaurés et le service fonctionne normalement), ils doivent envoyer une notification finale de l'incident.

Les CSIRT surveillent les réseaux afin de détecter les incidents éventuels à un stade précoce[27], de diffuser des alertes à leur sujet et de fournir des solutions pour atténuer leurs effets. Ces équipes doivent être la porte d'entrée des notifications d'incidents, ce qui permettra d'organiser rapidement la réponse à ces derniers.

La gestion des incidents de sécurité prendra en compte:

- **La mise en place de systèmes de détection et de réaction aux codes malveillants.**
- **L'enregistrement des incidents de sécurité qui se produisent et les actions de traitement qui sont suivies.**
- **Soutien et coordination pour le traitement des vulnérabilités et la résolution des incidents de sécurité.**
- **Fournir des informations sur les vulnérabilités, des alertes et des avertissements sur les nouvelles menaces. Comprend la recherche et la diffusion des meilleures pratiques en matière de sécurité de l'information.**
- **Formation pour améliorer les capacités de détection et de gestion des incidents.**

---

26. Les deux termes sont utilisés pour désigner une équipe d'experts en gestion d'incidents. ***CERT****: Computer Emergency Response Team y* ***CSIRT****: Computer Security Incident Response Team.* Le premier de ces termes est enregistré par CERT CC, la première équipe de ce type à l'Université Carnegie Mellon aux États-Unis.
27. Le système d'alerte précoce du CCN-CERT (SAT INET et SAT SARA) en est un exemple.

Un plan d'action de base contre un cyberincident peut être le suivant:

- **La DÉTECTION de la menace peut être effectuée par l'entité elle-même et/ou par les sondes déployées par l'équipe de réponse aux incidents cybernétiques (CSIRT) de référence, qui générera l'alerte correspondante.**

- **Dans le cas où le cyberincident est confirmé, l'agence effectue la notification officielle (par exemple, l'outil LUCIA) à l'autorité compétente, par l'intermédiaire du CSIRT de référence, et les actions de la phase de CONTENTION.**

- **Une fois la menace ERADICÉE, l'entité, à l'aide du même outil, notifie à l'autorité compétente, par l'intermédiaire du CSIRT de référence, la clôture du cyberincident.**

Figure 5. Schéma de base d'action en cas de cyber-incident

14. Politique de sécurité

La gestion des cyber-incidents (hiérarchisation et allocation des ressources, etc.) nécessite de déterminer le danger potentiel que présente le cyber-incident. Pour ce faire, il est nécessaire de fixer les critères de détermination du danger avec lesquels comparer les preuves disponibles au cyber-incident dans ses premiers stades.

15. Décalogue de sécurité de base

Ce décalogue de bonnes pratiques vise à jeter les bases de l'instauration d'une culture de la sécurité.

Décalogue de sécurité de base

1. La **culture de la cybersécurité**, la sensibilisation des employés, doit être l'un des piliers sur lesquels repose la cybersécurité de toute organisation.

2. **N'ouvrez** pas de lien ou ne **téléchargez** pas de pièce jointe à partir d'un courriel qui présente un **schéma inhabituel**.

3. L'utilisation de **logiciels de sécurité**, **d'outils anti-virus et anti-malware**, **de de pare-feu** personnels, **d'outils de suppression sécurisée**, devrait être une obligation lors de l'utilisation d'un **système TIC**.

4. **Limiter la zone d'exposition aux menaces**, non seulement en mettant en œuvre des mesures de sécurité qui protègent l'accès aux informations, mais aussi en déterminant les services qui sont strictement nécessaires.

5. **Cryptez les informations sensibles**, il n'y a pas d'autre solution.

6. Utilisez des **mots de passe** adaptés à la fonctionnalité en sachant que la double authentification est déjà une nécessité.

7. **Supprimez de manière sécurisée** les informations une fois qu'elles ne sont plus nécessaires ou que le support en question doit être mis hors service.

8. **Faites des sauvegardes régulières,** il n'y a pas d'alternative en cas d'infection par un code malveillant tel qu'un ransomware, de perte de données, de panne du matériel de stockage, de suppression involontaire d'informations par l'utilisateur, etc.

9. **Maintenir vos applications** et votre système d'exploitation à jour est le meilleur moyen d'éviter d'activer cette menace potentielle.

10. Examinez régulièrement les **paramètres de sécurité appliqués**, les **autorisations des applications** et les **options de sécurité**.

CCN centro criptológico nacional

CCN cert centro criptológico nacional

Figure 6. Décalogue de sécurité

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es