GUIDE DE SECURITE NUMERIQUE

A l'attention des responsables publics

SOMMAIRE

Avant-propos 3
Contexte 3
Glossaire 3
Internet 4
Téléphonie mobile 6
Tablettes 8
Poste de travail 8
Déplacements à l'étranger 9
Séparer les usages personnels des usages professionnels 10
Votre informatique personnelle 11
Gestion des mots de passe 12
Sécurité des données 13
L'ANSSI 15
En cas de problème 16
Contacts 17

Avant-propos

La sécurité des Systèmes d'Information revêt une importance capitale pour les individus et les Etats au regard des multiples menaces pesant sur leurs systèmes. Les responsables publics ont la lourde charge de protéger les actifs de l'État. Pour ce faire, ils doivent être informés des menaces, des risques existants et des mesures appropriées à prendre. En effet, les résultats et fruits des efforts entrepris par l'exécutif peuvent être annihilés par la compromission de ces systèmes d'information. Le présent document est un ensemble de bonnes pratiques destinées aux premiers responsables administratifs dans le cadre de l'exécution de leur mission.

Contexte

Ce guide est élaboré dans un contexte de menaces multiformes sur les systèmes d'information des Etats, des entreprises et des individus.

En effet, la recrudescence des malveillances connait un accroissement exponentiel, alors que des pays comme le Burkina Faso sont toujours aux prémices de la riposte à ces menaces dans un contexte de développement de l'économie numérique caractérisé par une rapide transformation digitale en cours, le déploiement des grands projets nationaux, la dématérialisation de la chaine des finances publiques et des autres actes administratifs, ainsi que l'essor du commerce électronique.

C'est pourquoi le gouvernement du Burkina Faso a créé une agence nationale chargée de la sécurité des systèmes d'information et qui a pour mission essentielle d'assoir un dispositif national de protection des actifs numériques face aux menaces cybernétiques.

Le présent guide a pour objectif de mettre à la disposition des premières autorités du pays un document de bonnes pratiques qui peut être exploité quotidiennement pour la sécurité de leur environnement de travail et de leur système d'information personnel.

Glossaire

Risque : il désigne la probabilité qu'une vulnérabilité soit exploitée par une menace causant des dommages à un actif. Il peut aussi se définir par la relation suivante, conjonction de trois facteurs : Risque = (Menace x Vulnérabilité) / (Contre-mesure)

Menace : une menace est une cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation. Elle désigne l'exploitation d'une faiblesse de sécurité par un attaquant, qu'il soit interne ou externe à l'entreprise.

Vulnérabilité : aussi être appelée ***faille***, ***défaut*** ou ***faiblesse*** ou ***brèche***, la vulnérabilité représente le niveau d'exposition face à la menace dans un contexte particulier.

Contre-mesure : ensemble des actions mises en œuvre en prévention de la menace. Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Virus : Programme malveillant destiné à endommager ou freiner le fonctionnement d'un système informatique.

Cheval de Troie : programme qui s'installe de façon frauduleuse pour remplir une tâche hostile à l'insu de l'utilisateur (espionnage, envoi massif de spams…).

Chiffrement : procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement.

Compte d'administrateur : compte avec des privilèges élevés permettant d'effectuer des modifications affectant les utilisateurs ou les ressources sensibles (modification des paramètres de sécurité, installation de logiciel, etc.).

Phishing (hameçonnage) : méthode d'attaque qui consiste à imiter les couleurs d'une institution ou d'une société (banque, services des impôts) pour inciter le destinataire à fournir des informations personnelles.

Internet

Tous les appareils connectés à internet sont susceptibles d'être attaqués. Ainsi, naviguer sur internet peut présenter des risques pour la sécurité des informations sensibles que vous traitez ou celle de vos données à caractère personnel. Des personnes malveillantes peuvent récolter vos informations personnelles à votre insu, afin par exemple de deviner vos mots de passe, vous tendre des pièges à l'aide de courriers électroniques personnalisés, d'accéder à votre système informatique, etc.

Des précautions peuvent être prises en respectant les bonnes pratiques en la matière et ainsi éviter une majeure partie de ces risques.

1) La navigation

1. Connexion à un Wi-Fi public : ne vous risquez pas à consulter des sites qui contiennent des informations confidentielles (mails, échanges professionnels,

banque en ligne) lorsque vous êtes connecté sur un réseau Wi-Fi public **:** si la connexion n'est pas sécurisée, ces informations peuvent être récupérées par des pirates ;

2. Dangers du compte administrateur : ne jamais se connecter avec un compte administrateur ; plutôt privilégier un compte utilisateur simple car un compte administrateur lègue tous vos droits (configuration de votre ordinateur, actions de hauts privilèges sur le réseau);

3. Sites malveillants : une visite sur un site web malveillant peut être source d'infection de votre ordinateur. Il est recommandé de cliquer donc uniquement sur des liens, des images et des vidéos pour lesquels vous avez confiance. Apprendre alors à reconnaître un site fiable à son adresse (URL).

4. Services gratuits : Une fois en ligne, « méfiance est mère de sûreté ». Il est alors recommander de se méfier d'applications, d'offres en ligne et de logiciels gratuits, de promesse de fortune, d'intermédiaire pour des transactions internationales.

5. Identité numérique : la plus grande prudence est conseillée dans la diffusion de vos informations personnelles à travers de multiples formulaires sur Internet, car ce que l'on publie sur Internet est quasi éternel et l'identité n'est jamais réellement secrète.

2) La messagerie

Dans l'utilisation courante, il existe quelques précautions à prendre :

1. À l'envoi

- ✓ Veillez à toujours vérifier l'adresse des destinataires et le niveau de confidentialité d'un message à envoyer et des documents joints ;
- ✓ Notamment prenez en considération l'historique des échanges inclus dans le message.

2. À la réception

- ✓ N'ouvrez pas les courriels non sollicités ou d'origine inconnue, même si l'objet ou la pièce jointe semble intéressant ;
- ✓ Méfiez-vous de toute pièce jointe à un courriel non sollicité ;
- ✓ Désactivez les fonctions de script dans les programmes de messagerie électronique ;
- ✓ Ne répondez jamais par mail à une demande d'information personnelle ou confidentielle ;
- ✓ Ne relayez pas les chaînes de messages (chaine de solidarité, fortune potentielle, bon ou mauvais sort, etc.) ;
- ✓ Désactivez l'ouverture automatique des documents téléchargés ;

- ✓ Ne téléchargez pas de données professionnelles sur des équipements communicants personnels ;
- ✓ Ne communiquez pas d'informations personnelles et confidentielles (et surtout pas de mot de passe). De manière générale, ces demandes, lorsqu'elles sont légitimes, ne se font jamais par courriel.

3. A retenir

- ✓ Ne transmettez jamais par le net une donnée hautement sensible ;
- ✓ Utilisez un canal crypté pour échanger les données confidentielles ;
- ✓ Classez les mails dans des dossiers spécifiques suivant l'expéditeur, l'objet, le contenu.

3) Les réseaux sociaux

Facebook, Twitter, Google+, YouTube, LinkedIn et d'autres réseaux sociaux sont devenus partie intégrante de notre vie en ligne. Les réseaux sociaux sont un excellent moyen de rester en contact avec les autres, mais il est recommandé de se méfier des informations personnelles publiées.

Les réseaux sociaux peuvent être source d'attaques informatiques : une connexion à une page contenant un code malveillant, souvent à l'insu de son créateur, peut compromettre votre smartphone, tablette ou ordinateur.

Des recherches sont parfois menées par des logiciels robots qui analysent vos écrits pour récupérer vos adresses de messagerie, vos identifiants et vos mots de passe afin de les réutiliser pour propager des courriels non sollicités. Par les cookies, vos habitudes de navigation (surtout les pages visitées) sont collectées par ces réseaux.

Apprenez à utiliser et vérifier régulièrement les paramètres de confidentialité et de sécurité pour vous protéger, garder vos informations personnelles, connaître et gérer vos amis, savoir quoi faire si vous rencontrez un problème.

Ne donnez accès qu'à un minimum d'informations personnelles et professionnelles sur les réseaux sociaux, et soyez vigilant lors de vos interactions avec les autres utilisateurs ; vos données renseignées pourraient faire l'objet de collecte par ingénierie sociale par des individus mal intentionnés usurpant votre profil et harcelant vos contacts.

Soyez conscient que toute connexion à un réseau social depuis un poste de votre organisme expose l'ensemble du système d'information à des risques d'attaque. Ne vous y connectez que si cela ne peut être évité et signalez à votre responsable informatique tout comportement suspect de votre équipement consécutif à une telle connexion.

Téléphonie mobile

La sécurité des communications à travers les opérateurs téléphoniques n'est toujours pas fiable quant aux critères de confidentialité :

- les réseaux et les équipements fixes utilisés pour les conversations téléphoniques sont susceptibles d'être interceptés par de multiples moyens (hertzien, branchement, piégeage, etc.) ;
- les protocoles utilisés sur internet servent de plus en plus au transport de la voix et de l'image qui sont donc susceptibles d'être victimes des mêmes attaques que tout échange d'informations sur internet.

Aussi, lorsque vous utilisez le réseau de téléphonie fixe de votre organisme, ne traitez pas de sujets comprenant des informations sensibles.

Bien que proposant des services innovants, les smartphones sont aujourd'hui très peu sécurisés.
Il est donc indispensable de leur appliquer certaines règles élémentaires de sécurité informatique :

Quelques règles :

1) N'installez que les applications nécessaires ; vérifier avant de les télécharger et installer, à quelles données elles pourront accéder (informations géographiques, contacts, appels téléphoniques…) ;
2) Désactivez les accès Bluetooth et Wi-Fi « intrusifs » ;
3) En plus du code PIN qui protège la carte SIM du smartphone, utilisez un mot de passe pour sécuriser l'accès au terminal ou configurez un verrouillage automatique ;
4) Effectuez des sauvegardes régulières sur des supports externes ;
5) Ne stockez pas de données sensibles sur des ordinateurs portables, des téléphones intelligents, des tablettes ou d'autres appareils mobiles;
6) Ne préenregistrez pas les mots de passe.

Certaines mises à jour peuvent également vous être proposées. Tenez compte de la présentation du message ou du site (nombreuses fautes d'orthographe, etc.). La précaution de base consiste à télécharger vos applications sur une plateforme officielle (Apple ou Android) et non sur des sites inconnus. Sur ces plateformes, le risque n'est pas nul, mais il est bien moindre.

Avoir à l'idée en tout temps :

1) N'abordez pas d'information de haute sensibilité lors de vos conversations ;
2) Ne consultez pas votre messagerie professionnelle sur vos terminaux mobiles personnels (la confidentialité des échanges n'est pas assurée) ;
3) Souvenez-vous que tout téléphone du commerce peut permettre de vous géo localiser à votre insu ;
4) Utilisez ou ayez en projet l'utilisation de smartphones sécurisés.

Tablettes

Alors que les PC portables sont beaucoup considérés pour la mise en place de solution d'anti-virus et d'anti-malware, les smartphones et tablettes sont en laisse bien que leur nombre augmente. L'idée selon laquelle l'on n'a pas besoin d'un anti-virus sur un terminal mobile est fausse car les menaces pour la sécurité des smartphones et tablettes sont réelles. Il n'y a donc pas une sécurité garantie quant à l'usage des tablettes du commerce pour leur connexion au système d'information de votre organisme. Il est toutefois souhaité de procéder toujours à la mise à jour vers les derniers systèmes d'exploitation.

Bien garder ses outils mobiles. Si vos données sont perdues, consultées ou compromises en raison de la perte ou de l'exposition d'un ordinateur portable, d'une tablette, d'un téléphone intelligent ou d'un autre appareil mobile, les dommages qui en résultent peuvent être beaucoup plus importants que le coût de remplacement.

Poste de travail

1) Ne travaillez pas sous des sessions « Administrateur » : Dans l'utilisation quotidienne de votre ordinateur (navigation internet, courrier, utilisation de logiciels bureautique…), un mode « utilisateur » est tout à fait suffisant.

2) Utilisez des mots de passe compliqués (minimum douze caractères, combinant majuscules, minuscules, chiffres et caractères spéciaux).

3) Configurez l'écran de veille des postes de travail de manière à ce que le poste soit verrouillé et protégé par un mot de passe après une période d'inactivité de 10 minutes ; ou verrouillez manuellement votre poste à chaque instant que vous vous y absentez, par la combinaison **CTRL+ALT+DEL** ou **Windows + L** (pour les PC), **CTRL+SHIFT+EJECT** (pour les ordinateurs Mac);

4) Désactivez l'exécution automatique des supports USB ;

5) Protégez l'accès à certains fichiers ou dossiers, par mot de passe ou en les cachant ;

6) Effectuez une mise à jour régulièrement du système et des applications : chaque système d'exploitation (Windows, MacOs, Android, iOS, etc.) ou chaque logiciel présente des vulnérabilités. Celles-ci sont corrigées une fois identifiées, lors des mises à jour proposées par les éditeurs. Configurez les mises à jour automatiques ;

7) Ayez un antivirus actif et à jour sur votre poste de travail ;

8) Effectuez des sauvegardes régulières ;

9) Chiffrez les données si nécessaire (sur clés USB, envoi de mails, sur ordinateurs) pour anticiper un éventuel cas de perte ou de vol.

- ***L'intranet administratif***

Pour transmettre ou traiter les informations professionnelles, il est privilégié d'opter pour le travail dans l'intranet administratif.

9 Déplacements à l'étranger

Utiliser un ordinateur portable, une tablette ou un smartphone en déplacement est une pratique courante mais c'est une menace supplémentaire pour les informations sensibles en cas de vol ou de perte.

- **Avant la mission**

- Si possible, faites usage de matériel dédié aux missions (ordinateurs, téléphones, supports amovibles contenant les dossiers utiles ou exclusivement destinés aux échanges, etc.). Ces appareils ne doivent contenir aucune information autre que celles dont vous avez besoin pour la mission ;
- Sauvegardez les données à emporter avant de partir, afin de pouvoir les récupérer au retour en cas de perte, de vol ou de saisie des équipements ;
- Emportez vos propres chargeurs ;
- Apposez un signe distinctif sur les appareils emportés et sur leur housse, afin de pouvoir les identifier et pouvoir s'assurer qu'il n'y a pas eu d'échange, notamment pendant le transport ;
- Evitez d'emporter des données sensibles non chiffrées : privilégiez, si possible, la récupération de fichiers chiffrés une fois arrivé au lieu de mission, par usage de solution VPN dédiée ou via une boîte de messagerie en ligne spécialement créée et dédiée au transfert des données chiffrées ;
- En cas de besoin d'amender les documents, dossiers lors des trajets, équipez l'écran de votre ordinateur d'un filtre de confidentialité, afin d'en interdire la lecture par les voisins ;
- Gardez à l'esprit que les téléphones peuvent être utilisés pour la géo localisation. A cet effet, il est recommandé d'éteindre ces appareils.

- **Pendant la mission**

- Rassurez-vous que vos outils soient dans un environnement physiquement sécurisé : gardez avec vous les appareils, supports et fichiers. Ne les laissez pas dans un bureau ou dans une chambre d'hôtel, même dans un coffre ;

- En cas d'obligation de vous séparer des appareils mobiles, retirez et conservez avec vous la carte SIM, l'éventuelle carte mémoire ainsi que la batterie ;
- Utilisez un logiciel de chiffrement pour les données, et ne communiquez surtout pas d'information confidentielle à partir du téléphone mobile ;
- Effacez régulièrement l'historique des appels et navigations (données en mémoire cache, cookies, mots de passe d'accès aux sites web et fichiers temporaires) ;
- En cas de perte ou de vol d'un équipement ou d'informations, informez immédiatement l'ANSSI ;
- N'utilisez pas les équipements qui ont été offerts avant de les avoir faits vérifiés par l'ANSSI, car ils peuvent contenir des logiciels malveillants ;
- Refusez la connexion d'équipements appartenant à des tiers à vos propres équipements ;
- Evitez de connecter ses équipements à des postes ou des périphériques informatiques qui ne sont pas de confiance. Faites attention aux échanges de documents.

➢ **Après la mission**

Tout particulièrement si votre équipement a échappé à votre surveillance :

- Changez les mots de passe qui ont été utilisés pendant le voyage, en cas du moindre doute sur leur compromission ;
- De retour, il est recommandé de ne pas connecter les appareils au réseau de votre organisme avant de les avoir soumis pour vérification, par le responsable informatique.

Séparer les usages personnels des usages professionnels

Rapporter du travail à la maison ou utiliser le même équipement pour un usage professionnel et un usage personnel sont des actions nécessitant d'être bien cadrées. Afin de minimiser l'effet de boule de neige suite à une immixtion de la vie privée et professionnelle, il est fortement recommandé de séparer ces deux usages:

☛ N'utilisez pas d'outils propriétaires de type Gmail, Yahoo, Skype, Dropbox, etc., pour des échanges professionnels. Plutôt privilégier l'utilisation d'une messagerie professionnelle dédiée, car il est primordial de pouvoir échanger de manière sécurisée. Ainsi, une messagerie professionnelle, basée sur le nom de domaine de la structure pourrait permettre d'avoir :

- un antivirus et anti spam inclus directement sur le serveur ;
- une offre robuste de messagerie avec des communications chiffrées de bout en bout ;
- une sauvegarde des mails effectuée directement sur serveur.

- Utilisez plusieurs adresses mail pour les multiples usages. En dehors du mail professionnel, il est recommandé d'avoir un mail dédié aux activités sérieuses (réseau d'amis ; transactions bancaires, etc.) et un mail notamment pour les activités de loisir (jeux, forums publics, autres divertissements);
- Ne transférez pas les messages électroniques professionnels vers une messagerie personnelle et inversement ;
- Ne traitez pas des documents professionnels sur sa machine privée et inversement ;
- N'utilisez pas de moyens personnels de stockage (clé USB, disque dur externe, cloud…) pour enregistrer les données professionnelles, et inversement.

Votre informatique personnelle

1) Point d'accès wifi

Wi-Fi publics : Faites attention aux réseaux Wi-Fi publics : ces réseaux sont pratiques afin de surfer brièvement en ligne ou de déterminer son emplacement avec le smartphone. Ils constituent cependant un lieu privilégié au vol de données importantes car l'on ignore généralement qui gère ces réseaux et comment ils sont sécurisés**.**

Wi-Fi à domicile : si le point d'accès n'est pas sécurisé, l'utilisation du Wi-Fi permet, à des personnes malintentionnées d'intercepter vos données et d'utiliser votre connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes. Pour sécuriser votre point d'accès Wi-Fi, il vous suffit de le configurer. Voici quelques recommandations générales :

- modifiez le nom d'utilisateur et le mot de passe par défaut de votre page de configuration accessible via un navigateur internet ;
- vérifiez que le point d'accès dispose du protocole de chiffrement WPA2 et l'activer (n'utilisez jamais le chiffrement WEP « cassable » en quelques instants);
- modifiez la clé de connexion par défaut par une clé de protection de plus de dix (10) caractères de types différents (alphanumériques et caractères spéciaux);
- ne divulguez la clé de connexion qu'à des tiers de confiance et changez-la régulièrement;
- activez et configurez les fonctions pare-feu/ routeur.

2) Télécharger les programmes sur les sites de leurs éditeurs

Les téléchargements sur des sites non officiels peuvent contenir des programmes malveillants (virus, ver, cheval de Troie, porte dérobée, logiciel espion, enregistreur de frappe) capables de compromettre la sécurité de votre système ou de vos données par prise de contrôle à distance de votre machine pour nuisance ou pour espionnage, ou alors pour mener une attaque. Dans ce contexte, afin de veiller à la sécurité de votre ordinateur et de vos données:

- il est fortement recommandé de télécharger des programmes uniquement sur les sites officiels des éditeurs ;
- désactivez les cases proposant d'installer des logiciels complémentaires ;
- restez vigilants concernant les liens sponsorisés ;
- désactivez l'ouverture automatique des documents téléchargés.

3) Etre prudent lors des achats en ligne

Avec un marché en croissance exponentielle et une augmentation des transactions en ligne, la sécurisation des données et des dispositifs de paiement constitue un critère fondamental pour mettre en confiance les consommateurs. Cependant, des précautions restent toutefois à prendre car les coordonnées bancaires peuvent être interceptées si le canal de paiement et/ou le site de transaction n'offrent pas des conditions sécurisantes. Il est alors demandé d'être vigilant lors d'un paiement sur Internet. A cet effet :

1) Contrôlez la présence d'un cadenas dans la barre d'adresse du navigateur Internet (notons que ce cadenas n'est pas visible sur tous les navigateurs) ;
2) Vérifiez que l'adresse du site commence par « **https** » et vérifiez de même la chaine de caractères de l'url pour déceler d'éventuelles fautes d'orthographe, révélant des sites malicieux ;
3) Privilégiez les achats comportant une confirmation de commande par SMS ou par mail ;
4) Ne communiquez jamais vos coordonnées bancaires par mail ou SMS et n'hésitez pas à consulter votre banque pour connaître les moyens sécurisés qu'elle propose.

Gestion des mots de passe

1) L'accès à un poste de travail informatique ou à un fichier par identifiant et mot de passe est la première des protections.

2) Un mot de passe doit comporter au minimum 8 (la nouvelle recommandation est de douze caractères) caractères incluant chiffres, lettres et caractères spéciaux et doit être renouvelé fréquemment (par exemple tous les 3 mois).

3) Le mot de passe doit être individuel, difficile à deviner et rester secret. Il ne doit donc être écrit sur aucun support et ne jamais être communiqué ;

4) N'utilisez pas le même mot de passe pour plusieurs comptes (mails, session Windows, banque, etc.) ;

5) Utilisez un logiciel de confiance de gestion de mot de passe et désactivez celui des navigateurs ;

6) Modifiez tous les éléments d'authentifications (identifiant et mot de passe) par défaut de vos équipements (imprimante, serveurs, modem Wi-Fi, etc.) ;

7) Modifiez immédiatement les mots de passe connus par une tierce personne.

Sécurité des données

Accès

1) Le premier effort de sécurité est d'imposer une barrière physique à leur accès et rendre disponible les données contre les aléas environnants. Veillez bien sur qui peut accéder directement à la machine ou indirectement à la donnée ;

2) Protégez l'accès aux données sensibles par un mot de passe fort ou, idéalement pour les données plus sensibles en les chiffrant directement sur le disque (ex. d'outils : VeraCrypt, Portable PGP, GnuPG, FileVault2) ;

3) Assurez un contrôle d'accès aux données respectant le principe du moindre privilège. Ne travaillez donc pas sous une session Administrateur.

4) Ne donnez pas d'informations personnelles sur le téléphone, par la poste ou sur Internet, sauf si vous êtes sûr de qui vous avez affaire.

Traitement

1) Ne laissez pas des données confidentielles directement sur votre bureau ;

2) Identifiez les données à protéger (données dont la divulgation porterait préjudice à votre activité, à la sureté de l'Etat, etc…) et veillez à leur protection en tout moment de leur chaine de traitement avec sa structure et celle des collaborateurs.

3) Les logiciels bureautiques ont un niveau de protection intégrée par mot de passe. Cette protection s'avère bien souvent suffisante pour un usage quotidien.

Sauvegarde

1) Conservez toutes les informations importantes et/ou confidentielles en lieu sûr (pas sur des disques durs locaux ou dans des dossiers publics d'Outlook Exchange) ;

2) Évitez de stocker les données uniquement sur un poste de travail, une clé USB ou un disque dur externe. Assurez-vous d'avoir plusieurs copies des données, en lieu sûr ;

3) Méfiez-vous des clés USB, disques durs externes, notamment si vous n'en êtes pas le propriétaire ;

4) Prêtez une grande attention aux médias externes (clés USB, disques durs externes, etc.) contenant des données confidentielles car ils sont plus faciles à copier ou à voler ;

5) Chiffrement des informations : pour limiter les conséquences aux vols, il est possible de chiffrer certaines informations que le support contient (disque dur, clé USB). Le chiffrement d'informations consiste à les rendre incompréhensibles à toute personne ne disposant pas de la clé de déchiffrement ;

6) Effectuez des sauvegardes quotidiennes ou hebdomadaires (en local ou sur support externe sécurisé) vous permettant de disposer de vos données en cas de dysfonctionnement du système informatique ou en cas d'attaque, de vol.

Transfert

1) Réalisez tout transfert de données sensibles vers l'externe en utilisant un canal de communication chiffré ou en chiffrant les données avant leur envoi (ex. d'outils : *VeraCrypt, Portable PGP, GnuPG, FileVault2*) ;
2) Évitez l'utilisation de services de stockage externe (ex. Dropbox) pour partager des données sensibles ;
3) Chiffrez les données sensibles, en particulier sur le matériel potentiellement perdable ;
4) Chiffrez les données sensibles transmises par voie Internet, ou à transférer dans le cloud ;
5) Protégez-vous des menaces relatives à l'utilisation de supports amovibles pour le transfert de données.

Suppression

1) Supprimez bien vos données : effectuez une élimination sécuritaire de toutes les données en format papier ;

2) Avant de jeter ou faire don d'un ordinateur, un smartphone, un disque dur ou une clé USB, veillez à supprimer efficacement (à l'aide de programmes spéciaux) les données enregistrées dessus, car les données sensibles n'étant pas supprimées de manière fiable peuvent être restaurées avec des programmes de récupération de données.

L'ANSSI

L'Agence Nationale de Sécurité des Systèmes d'Information **(**ANSSI) est un établissement public de l'Etat à caractère administratif, chargé de la gestion de la sécurité des systèmes d'information et du cyberespace du Burkina Faso, placé sous la tutelle technique du Premier Ministère et la tutelle financière du Ministère en charge des finances.
Elle est placée sous l'autorité d'un Directeur Général et s'articule autour des structures suivantes :

- la Direction Générale ;
- le Secrétariat Général ;
- les Directions techniques et administratives.

➢ MISSIONS

L'ANSSI est l'autorité nationale en matière de protection des systèmes d'Information. Elle a pour mission d'assurer la protection du cyberespace national.
A ce titre, elle est chargée notamment de :

- réduire la vulnérabilité du cyberespace national ;
- gérer les incidents de sécurité ;
- renforcer la culture de cybersécurité ;
- veiller à l'exécution des orientations nationales et de la stratégie nationale de cybersécurité;
- établir des normes spécifiques à la sécurité des systèmes d'information ;
- élaborer et publier des guides techniques et des référentiels;
- œuvrer au développement de solutions nationales dans le domaine de la sécurité des systèmes d'information et les promouvoir conformément aux priorités et aux programmes qui seront fixés par l'ANSSI ;
- participer à la consolidation de la formation et du renforcement des capacités dans le domaine de la sécurité des systèmes d'information ;
- accréditer les auditeurs de sécurité des systèmes d'information et des réseaux installés sur le territoire national ;
- suivre l'exécution des plans et des programmes relatifs à la sécurité des systèmes d'information et assurer la coordination entre les intervenants dans ce domaine ;
- assurer la veille technologique dans le domaine de la sécurité des systèmes d'information ;
- veiller à l'application de la règlementation relative à l'obligation de l'audit périodique de la sécurité des systèmes d'information et des réseaux installés sur le territoire national ;
- délivrer des agréments aux dispositifs et mécanismes de sécurité destinés à protéger les systèmes d'information ;
- coordonner aux niveaux régional et international les relations de l'agence avec ses partenaires extérieurs ;
- participer aux rencontres nationales et internationales sur la sécurité des systèmes d'information.

En matière de cybersécurité, l'ANSSI est chargée entre autres de la coordination des activités liées à la cybersécurité, la veille technologique en matière de système de sécurité, l'analyse de la menace, l'identification des vulnérabilités des systèmes et outils actuels, la recherche et la qualification des attaques en cours, la définition des mesures de réponse aux attaques, l'aide à l'application des mesures correctrices urgentes.

En cas de problème

Vous avez des questions sur la sécurité de vos équipements numériques, vous avez été victime ou témoin d'un incident, y compris la perte ou le vol d'un équipement (ordinateur, tablette, clé USB, etc.), tout signe d'intrusion, d'utilisation frauduleuse d'un ordinateur ou d'infraction de sécurité, ainsi que tout comportement inhabituel ou inattendu, contactez sans délai votre responsable informatique ou, en cas de compromission de données très confidentielles, s'adresser à l'ANSSI.

Contacts

06 BP 10 539 Ouagadougou 06
Tél. : 25 36 21 31 ou 25 36 32 33 **/** 25 37 53 60 (CIRT)
Mails : secretariat@anssi.bf **/** cirt@cirt.bf