FNAC DARTY

POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION (PSSI)

Modifications apportées par	Le	COMMENTAIRES
Corinne NOEL	27 Juin 2020	Revue 2020
Corinne NOEL	15 Avril 2021	Revue 2021

Table des matières

INTRODUCTION

a) CONTEXTE ET OBJECTIFS

Dans le secteur de la grande distribution, caractérisé par une priorité donnée à la réactivité opérationnelle, les enjeux liés au Système d'Information sont nombreux (satisfaction des clients, sécurisation des paiements, ouverture du SI aux tiers, etc.) et les risques potentiels ne cessent d'augmenter (disponibilité du SI, intégrité et confidentialité des informations de la clientèle, intelligence économique, etc.).

La présente Politique de Sécurité du Système d'Information (PSSI) définit pour l'ensemble de Fnac Darty les principes et les règles de sécurisation du Système d'Information. Ainsi, cette politique définit **une cible à atteindre en termes de Sécurité du SI**.

Afin d'assurer une cohérence avec les pratiques actuelles en terme de sécurité, la PSSI est fondée sur les normes ISO27001 et ISO27002.
Dans cette version de la PSSI, et pour traiter l'essentiel, nous avons convenu de ne retenir que les mesures de sécurité correspondant aux risques « quasi certains » et « plausibles ».

b) LES ENJEUX DE LA SECURITE DU SYSTEME D'INFORMATION

Dans ce contexte, l'enjeu majeur de la PSSI est la protection du patrimoine informationnel de Fnac Darty au regard des critères de **Disponibilité, Intégrité, Confidentialité, Traçabilité et de Conformité légale et réglementaire** qui constituent le fondement d'une démarche sécurité.
La Sécurité du Système d'Information a pour objectif de répondre à plusieurs enjeux importants :

- **Assurer la continuité** des services rendus, à travers celle des processus métiers.

  Exemples : La disponibilité des référentiels de données (articles, fournisseurs, ventes, tarifs), et la continuité des processus clés (approvisionnement, encaissement, paye des collaborateurs, règlement des fournisseurs, etc.) sont essentielles au bon fonctionnement des activités de Fnac Darty. Des pertes d'exploitation directes et indirectes seraient inévitables en cas d'interruption de ces services.

- **Assurer le respect des obligations légales**, réglementaires et contractuelles. Le Système d'Information doit contribuer au respect de ces obligations. Leur non-respect est susceptible d'engager la responsabilité de Fnac Darty et de ses dirigeants.

  Exemples : Fnac Darty se doit notamment

  - De ne pas divulguer les données à caractère personnel qu'il héberge sauf en cas de déclaration ad hoc (clients, collaborateurs, fournisseurs, partenaires, etc.) : données bancaires, coordonnées, habitudes de consommation, etc.
  - De respecter la loi en matière de propriété intellectuelle (utilisation de logiciels avec licence acquise légalement, dépôt des noms de domaine des sites Internet Fnac Darty, etc.).
  - De se protéger contre les usages frauduleux ou illégaux de ses Systèmes d'Information (piratage, harcèlement, apologie de crimes contre l'humanité, incitation à la haine raciale, pédophilie, etc.).

- **Protéger le patrimoine matériel et immatériel** (informations, données, etc.) contre les risques de malveillance, d'erreur et d'accident.

  Exemples :

  - La divulgation d'informations stratégiques à la concurrence (conditions d'achat, plan commercial, plan d'expanSIon, etc.) ainsi que les données personnelles peut constituer un préjudice grave
  - L'altération de données empêchant d'attribuer les avantages clients ou la fraude potentielle sur les cartes de fidélités peut se traduire par une perte financière directe ou une perte de clientèle.

- **Préserver la confiance des clients, des collaborateurs, des actionnaires, des fournisseurs, des partenaires**. Les défauts de Sécurité du SI perceptibles de ces acteurs sont susceptibles de porter atteinte à leur confiance et à leur fidélité à Fnac Darty.

  Exemples :

  - La divulgation d'informations appartenant aux clients ou l'usage abusif de ces informations, si elles sont divulguées dans la presse, peut gravement entamer la confiance d'une partie de la clientèle.
  - Le Système d'Information doit donc s'inscrire dans une démarche explicite de maîtrise des risques et de gestion de la sécurité de l'information, afin de protéger les activités et le savoir-faire de Fnac Darty de manière proportionnée aux enjeux, tout en gardant la maîtrise des coûts induits.

c) ORGANISATION DOCUMENTAIRE

Le référentiel de Sécurité du Système d'Information est composé d'un ensemble de documents :

- **Le document de Politique de Sécurité du Système d'Information de Fnac Darty** : Ce document doit être connu de l'ensemble des acteurs internes à la société, ainsi que de l'ensemble des prestataires et sous-traitants pour ce qui les concerne. Il permet de formaliser et de rendre accessible aux différents acteurs des métiers et de la Direction Organisation des systèmes d'Information (DOSI), les politiques, organisations, règles, normes, standards et procédures applicables à la gestion de la sécurité du Système d'Information de Fnac Darty.

- **La charte d'utilisation du Système d'Information** : Ce document s'adresse aux différents utilisateurs du Système d'Information de Fnac Darty. Il a pour objectif d'engager la responsabilité de tous les utilisateurs et de les informer de leurs devoirs et de leurs obligations.

- **Les Directives techniques et opérationnelles des mesures de sécurité définies sur les environnements de production** :
  - Le document CSD sur le périmètre IBM
  - Document de sécurité paratagé avec les partenaires et prestatires

- **L'analyse de risques SI** : Elle permet d'identifier quelles sont les mesures techniques et organisationnelles appropriées à prendre au regard des objectifs de sécurité que l'on s'est fixé notamment. Elle est conduite annuellement et intègre les éléments de réponses du questionnaire de mesure de la Sécurité.

d) PERIMETRE ET MISE EN APPLICATION DE LA PSSI

La PSSI s'applique à l'ensemble des entités interconnectées au réseau de Fnac Darty. Cela concerne notamment les **magasins**, le **siège**, les **filiales et entités opérationnelles de Fnac Darty** et les **tiers** (ex : affiliés, fournisseurs, infogéreurs etc...).
Les entités chargées des relations contractuelles et/ou opérationnelles avec les acteurs pré cités doivent s'assurer de la conformité de leurs pratiques avec la PSSI.
Les contraintes légales s'appliquent à toutes les filiales de Fnac Darty, sauf si des dispositions locales ne le permettent pas. Les spécificités locales ne sont pas traitées dans ce document.

e) LES PRINCIPES CLES DE LA PSSI

Principe n° 1 : La PSSI énonce les objectifs, ce qu'il faut obtenir en terme de résultats de sécurité et non comment l'obtenir.

Principe n° 2: La PSSI a l'appui de la Direction

Principe n° 3: La PSSI est contrôlable.
Les objectifs de sécurité doivent être clairs, précis et justifiables, de manière que la mise en œuvre soit contrôlable et qu'une « métrique », essentiellement des indicateurs associés aux objectifs de sécurité (appelés « tableau de bord ») puissent permettre de juger du niveau réel de la SSI.

Principe n° 4 : la PSSI est évolutive
La PSSI est évolutive et doit être révisée en fonction des enseignements tirés de l'expérience passée, de l'évolution de l'environnement, des process et organisation de Fnac Darty, sans oublier du contexte (évolution des menaces, évolution de la réglementation, de la jurisprudence).

Principe n° 5 : savoir gérer les exceptions !
Quelle que soit la PSSI adoptée, il faut savoir gérer les exceptions ou dérogations aux principes de sécurité. Toutefois, ces exceptions ne doivent pas devenir la règle ; elles font l'objet d'un référencement et doivent être revues annuellement.

Principe n° 6 : la PSSI est un document pédagogique
Une PSSI n'a aucune chance d'être appliquée SI elle n'est pas comprise et partagée.

ORGANISATION ET PILOTAGE DE LA PSSI

Fiche n°1 . ANALYSE DE RISQUES SI

Définition

Un risque est un scénario qui combine une situation crainte (par exemple atteinte de la sécurité des traitements et ses conséquences) avec toutes les possibilités qu'elle survienne (par exemple menaces sur les supports des traitements). On estime son niveau en termes de gravité (ampleur et nombre des impacts) et de vraisemblance (possibilité/probabilité qu'il se réalise).

L'analyse des risques permet d'identifier quelles sont les mesures techniques et organisationnelles appropriées à prendre au regard des objectifs de sécurité que l'on s'est fixé notamment

- S'assurer de la continuité des services rendus, à travers celle des processus métiers.
- S'assurer du respect des obligations légales, réglementaires et contractuelles
- Protéger le patrimoine matériel et immatériel (informations, données, etc.) contre les risques de malveillance, d'erreur et d'accident.
- Préserver la confiance des clients, des collaborateurs, des fournisseurs, des partenaires et des actionnaires. Les défauts de Sécurité du SI, perceptibles de ces acteurs, sont susceptibles de porter atteinte à leur confiance et à leur fidélité.

Risques

- Non connaissance des risques informatiques qui pèsent sur l'activité de l'entreprise.
- Pas de vision globale du Système d'Information.
- Inadéquation des exigences sécurité avec les enjeux stratégiques de Fnac Darty.

Règles

Analyse de risques SI
Une analyse de risques SI doit être conduite annuellement dans le cadre d'une démarche globale groupe Fnac Darty. Elle doit garantir une identification, une quantification des risques (IMPACT versus GRAVITE) et une analyse de réduction (cours et moyens termes) de ces derniers. Elle est basée sur une démarche ISO et intègre toutes les obligations contractuelles et réglementaires. L'analyse des risques SI sera intégrée à la cartographie standardisée des risques, exercice mené annuellement par la Direction de l'Audit Interne.

Budget de sécurité
Les Responsables de la DOSI doivent prévoir les budgets informatiques nécessaires à la remédiation des risques en fonction du mode de traitement défini en Comité de Sécurité (refus, optimisation, transfert ou prise de risque)

Fiche n°2 . COMITES DE SECURITE SI

Définition

Les Comités de Sécurité doivent être représentatif de l'ensemble des acteurs de la DOSI.
Ils permettent d'engager un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein du SI Fnac Darty, en interne mais aussi avec tous les partenaires externes du SI.
Ils sont animés par le Directeur de la sécurité des Systèmes d'Information avec l'équipe RSSI (responsable de la sécurité du SI) et composés en fonction du périmètre à couvrir.

Risques

- Non reconnaissance et non prise en compte de la démarche sécurité dans les activités quotidiennes des acteurs opérationnels du Système d'Information de Fnac Darty.
- Mauvaise vision des actions sécurités menées par la Direction SSI dans les différents projets de la DOSI.

Règles

Comité de Sécurité DOSI
Le Comité doit se réunir à l'initiative de la Direction de la sécurité du SI périodiquement et au minimum 3 fois par an. Il doit : - prendre connaissance des actions menées par les RSSI, - prendre connaissance des incidents de sécurité entre deux Comités, - prendre connaissance de la cartographie des risques - déterminer le mode de traitement des risques SI (refus, optimisation, transfert ou prise de risque) - suivre les exceptions de sécurité (mesures de sécurité non conformes mais acceptées) - arbitrer en cas de litige sur la mise en œuvre d'une mesure de sécurité, - analyser et valider les orientations sécurité proposées par la Direction de la SSI

Comité de Sécurité avec les partenaires
Chaque Comité doit se réunir périodiquement et au minimum 2 fois par an. Il doit : - Bilan du plan de traitement des risques et du plan d'actions - Indicateurs sur les mesures de sécurité - Evolution du périmètre, évolution des enjeux internes et externes, règlementaires - Historique des incidents majeurs et retours d'expérience - Opportunités d'amélioration continue

Fiche n°3 . ORGANISATION DE LA FONCTION SECURITE

Définition

L'organisation de la fonction sécurité dépend de la prise en compte des enjeux de sécurité par tous et de facto, au respect et à la déclinaison des règles de sécurité de la PSSI.
Elle repose autour des acteurs suivants :

- ✓ Le DOSI, Directeur de l'Organisation et des Systèmes d'Information,
- ✓ Le Directeur de la Sécurité des Systèmes d'Information
- ✓ Les acteurs de la Direction Organisation et Systèmes d'Information (DOSI),
- ✓ Les Directions Métiers de Fnac Darty,
- ✓ Les directions « transverses » (Direction Juridique, Direction des Ressources Humaines, Direction Prévention des risques, Direction Audit etc.) en rôle d'appui,
- ✓ Les utilisateurs du SI.

Risques

- ❑ Absence de prise de conscience des risques liés au Système d'Information.
- ❑ Absence de prise en charge des besoins et des objectifs de sécurité du SI.
- ❑ Inadéquation entre les objectifs de sécurité et le niveau de sécurité du SI.

Exigences

Légitimité de la PSSI
La PSSI doit être supportée par la Direction de Fnac Darty et reconnu par l'ensemble des Directions et utilisateurs du SI Fnac Darty.

Responsabilité et objectifs de sécurité
Chacun doit veiller au respect de la PSSI dans l'ensemble des projets liés au SI et de l'exploitation du SI

Mise à jour de la PSSI
La PSSI doit être cohérente avec les objectifs de sécurité de l'entreprise et la stratégie globale de l'entreprise. Le RSSI doit faire une revue et une mise à jour SI nécessaire, de la présente PSSI et notamment à chaque : ❑ modification majeure du Système d'Information, d'évolutions majeures des process ou de l'organisation, ❑ modification des objectifs de sécurité de l'entreprise, ou à l'apparition d'une nouvelle réglementation ou de nouvelles menaces.

SECURITE DES RESSOURCES HUMAINES

FICHE N°4 . SECURITE DES RESSOURCES HUMAINES

Fiche n°4 . SECURITE DES RESSOURCES HUMAINES

Définition

Les processus liés au personnel contribuent à renforcer la sécurité, en considérant la sécurité pendant le recrutement, dans l'exécution des contrats de travail, des contrats avec les parties tierces, dans les programmes de formation et dans les procédures disciplinaires.

Risques

- Ne pas être en mesure de maintenir un système de management des ressources humaines stable qui est adapté à leurs conditions et assurant la disponibilité, l'intégrité et la confidentialité des informations relatives aux activités traitées par les ressources humaines.
- Ne pas s'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétent pour remplir les fonctions que le groupe envisage de leur confier.

Exigences

Avant l'embauche
La direction des ressources humaines s'assure que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier.

Gestion des nouveaux arrivants
La direction des ressources humaines communique aux nouveaux arrivants et utilisateurs du système d'information, le règlement intérieur avec en annexe la charte du bon usage du Système d'Information. Les vérifications de sécurité sont proportionnées aux exigences métiers et aux risques identifiés.

A la fin du contrat ou en cas de changement d'emploi
La direction des ressources humaines s'assure que les signataires concernés quittent l'organisation ou changent d'emploi de manière organisée. En cas de départ de l'organisation, la DOSI vérifie que tout l'équipement est retourné et que les droits d'accès ont été révoqués.

Mobilité et télétravail
La direction des ressources humaines met en œuvre des contrats spécifiquent au télétravail précisant les modalités et la fréquence. Le signataire atteste avoir une connexion internet haut débit ainsi que d'un espace de travail spécifique, lui permettant d'assurer son activité et à être joignable dans les mêmes conditions que lorsqu'il travaille dans les locaux de l'entreprise. La DOSI met en œuvre une solution de type Vpn, adaptée à son besoin et conforme aux régles de sécurité du SI.

Procedure disciplinaire
Un processus disciplinaire formel et connu de tous permet de prendre des mesures à l'encontre de tous les utilisateurs du SI ayant enfreint les règles liées à la sécurité de l'information.

Mise en place de mesures de sensibilisation à la sécurité des SI
La Direction de la SSI communique régulièrement sur les risques liés à la sécurité du SI et les bonnes pratiques en matière de sécurité de l'Information en menant des actions de sensibilisation via l'intranet, la messagerie ainsi que des campagnes d'affichage.

GESTION DES ACTIFS

Fiche n°5 . CLASSIFICATION ET GOUVERNANCE DES DONNEES

Définition

La classification des données consiste à qualifier les données en termes de Disponibilité, Intégrité, Confidentialité, Traçabilité, Archivage et Durées de Conservation. On parlera de gouvernance des données.

Risques

- Mauvaise utilisation de la donnée.
- Détournement de la donnée.
- Usurpation de la donnée.
- Perte de fiabilité de la donnée.

Exigences

Niveau de sécurité attendu en fonction de la classification

	Niveau 1 sécurité standard	Niveau 2 sécurité moyenne	Niveau 3 sécurité forte
Disponibilité	D1 L'information est accessible dans un délai inférieur à 2 jours.	D2 L'information est accessible dans un délai inférieur à 8h	D3 L'information est accessible dans un délai inférieur à 4h
Intégrité	I1 Une perte d'intégrité pendant la période d'utilisation est suivie soit d'une détection facile puis d'une correction, soit d'une absence de perturbation significative du service rendu.	I2 L'altération d'une Information est impossible au cours de son utilisation. Seules les personnes autorisées peuvent la modifier.	I3 L'altération d'une Information est impossible au cours de son utilisation. Seules les personnes autorisées peuvent la modifier.
Confidentialité	C1 L'information est peu confidentielle. Elle est accessible à toute personne ayant accès à cet élément du si.	C2 L'information est confidentielle (diffusion contrôlée). Elle n'est accessible qu'aux personnes identifiées et habilitées	C3 L'information est masquée et chiffrée en base .
Traçabilité	T1 L'accès aux ressources n'est pas nécessairement journalisé. Les journaux d'évènements ne sont pas exploités systématiquement.	T2 L'accès aux ressources est journalisé. Les journaux d'évènements sont exploitables et conservés pendant 6 mois.	T3 L'accès aux ressources est journalisé. Les journaux d'évènements sont exploitables et conservés pendant 6 mois.
Durée de conservation	A1 Les durées de conservation ne sont pas soumises à une réglementation particulière.	A2 Les durées de conservation dépendent de dispositions légales définies ou déclarées auxquelles il faut se conformer . Des purges sont définies.	A3 Les durées de conservation dépendent de dispositions légales définies ou déclarées auxquelles il faut se conformer . Des purges sont définies.

Données confidentielles de Fnac Darty
Les données personnelles des clients ou salariés, informations qui permettent d'identifier directement ou indirectement une personne physique, sont des données confidentielles de niveau 2 minimum.

Propriétaire et Gouvernance des données
Toute donnée doit être attribuée à un responsable de traitement et doit faire l'objet d'une classification en termes de Confidentialité, d'Intégrité, de Disponibilité, de Traçabilité et de durée de conservation conformément à la réglementation en vigueur.

Marquage et manipulation des actifs
Il convient de respecter le plan de classification spécifiant comment manipuler, traiter, stocker et communiquer l'information en fonction de sa classification. Les actifs sont inventoriés et catégorisés par criticité dans les outils de référencement de la DOSI (tous périphériques , matériels gérés par les équipes Fnac Darty) ; Les documents contenant des informations de niveau 2 et plus doivent être clairement identifiés par une annotation de type «Confidentiel – ne pas diffuser»

Fiche n°6 . GESTION DES BIENS

Définition

La gestion des biens a pour but d'inventorier et de suivre l'ensemble des ressources informatiques dans leur cycle de vie (achat, attribution, capacité, panne, restitution, recyclage et mise au rebut).

Risques

- Mauvaise gestion des stocks
- Mauvaise attribution de la ressource.
- Perte de la ressource.
- Perte de fiabilité des inventaires.

Exigences

Inventaire
Il convient de clairement identifier tous les biens, de réaliser et de gérer un inventaire de tous les actifs informatiques, notamment : ❑ équipements informatiques (serveurs, ordinateurs, imprimantes, routeurs, pare-feu, etc...) ❑ applications et logiciels (systèmes d'opérations, base de données, middleware, outils de sauvegarde et surveillance, …), ❑ licences d'utilisation.

Restitution des biens en fin de contrat
Il convient que tous les salariés, contractants et utilisateurs tiers restituent la totalité des biens de l'organisme qu'ils ont en leur possession à la fin de leur période d'emploi, contrat ou accord.

Mise au rebut ou recyclage
Les composants disposant d'un mécanisme de stockage, doivent faire l'objet d'un Effacement couche basse avant réutilisation ou mise au rebut.

GESTION DES ACCES

Fiche n°7 . CLASSIFICATION DES PROFILS ET ACCES

Définition

La classification des profils a pour but de recenser l'ensemble des personnes présentant des exigences communes en matière de sécurité afin de créer des profils d'utilisateurs avec des droits et un degré de sensibilité associés.
L'entité propriétaire des données applicatives doit définir les droits d'accès aux données correspondant à chaque profil.

- Utilisateurs Métiers
- Responsables Métiers
- Administrateurs DOSI
- Etc …

Ainsi que la politique d'attribution.

Risques

- Attribution de droits excessifs non justifiées.
- Accès à des données non autorisées.

Exigences

Classification des profils
L'entité propriétaire des données applicatives doit définir des profils d'accès, permettant aux utilisateurs d'exercer leur métier et pas d'avantage. Il ne doit pas permettre de cumuler des fonctions incompatibles.

Politique d'attribution utilisateurs et séparation des tâches
L'entité propriétaire des données applicatives doit définir les politiques d'attribution des comptes et profil d'accès dans une logique de séparation des tâches dans le but de prévenir les risques de fraude et/ou de modifications illicites.

Fiche n°8 . COMPTE D ACCES

Définition

Un compte d'accès est la capacité de se connecter de manière unique et non équivoque au SI Fnac Darty

Risques

- Impossibilité d'affecter physiquement une action ou une ressource à un utilisateur.
- Usurpation d'identité.
- Accès non autorisé aux ressources du système d'information.

Exigences

Identification personnelle

L'identification d'un compte d'accès doit être nominative et personnelle.
Ainsi, il est rigoureusement interdit :

- D'utiliser des comptes autres que ceux auxquels l'utilisateur a légitimement accès (par exemple : utiliser un identifiant appartenant à une autre personne, même avec l'accord de ladite personne),
- De permettre l'utilisation de son propre compte à une tierce personne,
- D'essayer de masquer sa véritable identité.

Durée de validité des comptes d'accès

La durée de validité du compte d'accès doit correspondre au type de contrat de l'utilisateur (personnel interne, temporaire, etc.) et doit pouvoir être prolongée ou réduite.

Nomenclature des comptes

La nomenclature de l'identifiant ou login doit permettre le rapprochement quant à son propriétaire ou sa fonction.
Dans ce cadre,

- Un compte utilisateur doit être nominatif et permettre l'identification de l'utilisateur.
- Un compte applicatif et/ou de service doit être clairement identifiable en permettant le rapprochement quant à sa fonction ou l'application.
- La nomenclature en vigueur est respectée selon la Directive Technique DOSI - PSSI / Compte et mot de passe

Demande de réinitialisation du mot de passe
Le support utilisateur ne prend pas en compte les demandes de réinitialisation de mot de passe par téléphone. Une demande écrite est nécessaire par e-mail ou via le portail des services DOSI.

Comptes d'accès avec droits forts
Les comptes d'accès avec droits forts notamment administrateur, ne doivent pas être utilisés pour l'accès au poste de travail, seulement pour les tâches courantes d'administration. Ce principe implique la création aussi d'un compte utilisateur (sans droits forts) pour les administrateurs.

Comptes de services
Les comptes de services ne peuvent être utilisés que par des traitements systèmes et applicatifs. L'utilisation des comptes de service dans le cadre d'un accès personnel est interdite.

Attibution des accès
Une procédure de gestion des accès des comptes du domaine et applicatifs, existe et appliquée. Les accès et habilitations sont délivrées sur la base des fonctions métiers exercées. Les demandes d'accès aux ressources (fichiers, applications…) sont faites par les supérieurs hiérarchiques de l'utilisateur concerné. Aucun accès n'est accordé sans validation d'un supérieur ou du responsable fonctionnel

Requalification des accès lors de mouvement de personnel
Il convient que les droits d'accès de l'ensemble des utilisateurs (internes, externes) soient requalifiés en cas de changement de mission ,fonction ou périmètre. Pour ce faire, le responsable hiérarchique doit aviser la DOSI lors de tout mouvement de personnel.

Gestion des durées de validité des comptes d'accès
Il convient que les droits d'accès de l'ensemble des utilisateurs (internes, externes) correspondent au type de contrat de l'utilisateur (CDI, CDD ,3 mois pour les externes, etc…) Pour ce faire, le responsable hiérarchique doit aviser la DOSI lors de tout départ de personnel.

Fiche n°9 . POLITIQUE DE MOT DE PASSE

Définition

L'authentification d'un utilisateur est la preuve de son identité par sa capacité à être le seul à connaître son mot de passe

Risques

- Usurpation d'identité.
- Accès non autorisé aux ressources du système d'information.

Exigences

Confidentialité du mot de passe
Un mot de passe (ou authentifiant) est une information confidentielle. A ce titre, il ne doit jamais être écrit ou transmis, même de façon provisoire. (i.e. ne jamais communiquer son mot de passe, même au support utilisateurs ou aux administrateurs).

Composition des mots de passe
Les mots de passe utilisés doivent être composés de 10 caractères minimum (si l'application le permet) comprenant des majuscules, minuscules, chiffres et/ou caractères spéciaux. Les comptes nominatifs doivent être personnalisés à la première connexion.

Chriffrage des mots de passe
Les mots de passe doivent être chiffrés en base avec un algorithme, au minimum, SHA 256 avec sel qui devra faire l objet d'un stockage sur un espace distinct de celui où sont stockés les mots de passe.

Politique de changement de mot de passe
La politique de changement de mot de passe en vigueur (changement tous les 90 jours) s'applique sur tous les comptes utilisateurs. Il n'y a pas de dérogations pour les administrateurs dans la mesure où ceux –ci se doivent d'être exemplaires compte tenu des risques qu'ils feraient peser sur l'entreprise par la divulgation du mot de passe d'un compte avec droits forts. Les comptes de service/applicatifs n'étant pas soumis au changement de mot de passe sont inventoriés dans le cadre de la gestion des exceptions.

Mots de passe par défaut
Les mots de passe par défaut sont interdits. Les mots de passe donnés par le constructeur ou l'éditeur de la ressource informatique, doivent être changés en respectant le nombre de caractère minimum et le principe de complexité du mot de passe.

Fiche n°10 . DELEGATION DES DROITS

Définition

La délégation des droits est un processus qui a pour finalité de permettre à un détenteur de droits de déléguer ses droits, en particulier pour permettre d'assurer la continuité de service. La délégation de droit est obtenue par attribution des droits du profil du délégant au profil du délégué. Il ne s'agit en aucun cas d'une divulgation du compte et de son mot de passe.

Risques.

- Usurpation d'identité.

Exigences

Délégation de droits et compte d'accès
La délégation de compte d'accès doit permettre au délégué l'accès aux droits du délégant sans pour autant communiquer le compte et mot de passe du délégant. Elle implique obligatoirement la mise en place d'une traçabilité des accès au minima, idéalement une traçabilité applicative via les logs de connexion et applicatives. Il est recommandé d'utiliser la délégation disponible à travers les applications dans la mesure où elle permet d'en assurer le périmètre, la réversibilité, la limite dans le temps ainsi que la traçabilité.

Délégation des droits de réinitialisation de mots de passe
La délégation des droits de réinitialisation de mot de passe de compte d'accès peut être déléguée à une catégorie d'utilisateurs qu'après acceptation et validation auprès du responsable applicatif des données et aux RSSI. Elle implique obligatoirement la mise en place d'une traçabilité des accès au minima, une traçabilité applicative permettant d'identifier l'auteur d'une réinitialisation et sur quel compte, quand l'application le permet.

CRYPTOGRAPHIE

FICHE N°11 . CRYTOGRAPHIE

Fiche n°11 . CRYTOGRAPHIE

Définition

La gestion de clés de chiffrement, tout au long de leur cycle de vie, exige de stocker, archiver,retrouver, distribuer, désactiver et détruire ces clés.

Risques.

- Divulgation de données sensibles pour le groupe.

Exigences

Politique de chiffrement
Les informations en fonction de leur sensibilité doivent être chiffrées pendant leur transport et leur stockage ainsi que l'ensemble des flux trasitant en dehors du réseau interne

Gestion des clés
Une procédure de gestion des clés de chiffrement, de renouvellement et de stockage de certificats, existe et est appliquée.

SECURITE PHYSIQUE ET ENVIRONNEMENTALE

FICHE N°12 . SECURITE PHYSIQUE

Fiche n°12 . SECURITE PHYSIQUE

Définition
Il s'agit d'un ensemble de mesures visant à garantir la protection physique des locaux informatiques afin de garantir la confidentialité, la disponibilité et l'intégrité des données.

Risques

- Indisponibilité de tout ou partie du système d'information Fnac Darty
- Destruction physique ou dégradation d'un matériel informatique
- Vol d'un matériel informatique
- Accès physique non autorisé à un matériel informatique

Exigences

Contrôle d'accès physique aux salles informatiques
Les accès aux salles informatiques sont restreints uniquement aux personnes habilitées. Les salles informatiques sont équipées d'un dispositif de contrôle d'accès physique. Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones sensibles, intervient systématiquement et impérativement sous surveillance permanente.

Contrôle d'accès physique aux batiments
Le contrôle d'accès des salles informatiques pour le personnel du groupe s'appuie sur un système de contrôle par badges. Les moyens généraux fournissent un badge aux nouveaux arrivants, conformément aux habilitations d'accés nécessaires à leur mission. A chaque mouvement et réaffectation de poste, le badge est mis à jour pour correspondre aux habilitations requises de l'utilisateur.

Protection des locaux
Tous les moyens nécessaires - à la détection contre l'intrusion, - à la détection incendie et dégâts des eaux, - à la fourniture électrique, climatisation et télécommunication, doivent être mis en œuvre contre les désastres naturels, contre les attaques malveillantes ainsi que contre les accidents.

SECURITE LIEE A L EXPLOITATION

Fiche n°13 . SECURITE DU POSTE DE TRAVAIL

Définition

Il s'agit de définir les exigences de sécurité applicables aux postes de travail fixes et mobiles, permettant à un utilisateur d'accéder au SI de Fnac Darty.

Risques

- Accès non autorisé aux ressources informatiques de l'utilisateur pouvant entraîner un détournement de données stratégiques pour l'entreprise, une corruption de ces données ou leur destruction
- Introduction de codes malicieux (virus, chevaux de Troie, etc…) au niveau du SI Fnac Darty

Exigences

Droits sur le poste de travail
Les droits utilisateurs ne doivent pas permettre de modifier les éléments sensibles de la configuration ni même d'installer des applications. Seuls les administrateurs (Production) de la DOSI ont les pleins droits d'administration.

Installation de logiciels et de matériels
L'installation de logiciels, de matériels ou d'équipements mobiles et multimédia par les utilisateurs n'est pas autorisée, sauf cas exceptionnel et sous couvert d'une validation par le service informatique.

Respect des mécanismes de sécurité
La désactivation des mécanismes de détection des virus et descente automatique des patchs de sécurité sont interdites et doivent être rendues impossible par l'utilisateur.

Mode veille
Le mode veille de chaque poste doit être activé, doit revenir automatiquement en mode protégé en cas d'inactivité de 20 minutes et nécessite la saisie du mot de passe du compte d'accès (authentification Active Directory) au poste de travail.

Fiche n°14 . SECURITE DES EQUIPEMENTS MOBILES

Définition

Il s'agit de décrire les mesures complémentaires de sécurité, induites lors de l'utilisation d'équipements mobiles (poste de travail mobile, tablettes, Smartphones, etc …) contenant ou accédant à une partie du système d'information Fnac Darty. Ces composants doivent disposer d'un niveau de sécurité renforcée.

Risques

- Destruction physique ou détérioration d'un composant mobile
- Vol de composant mobile
- Accès non autorisé au système d'information à partir d'un composant mobile.

Exigences

Protection des équipements mobiles
Chaque utilisateur doit prendre toutes les précautions nécessaires pour protéger les équipements mobiles et leurs accessoires qui lui sont affectés. Il doit mettre en œuvre, lorsque cela est nécessaire, les moyens de sécurité mis à sa disposition. Les équipements mobiles ne doivent jamais être laissés sans surveillance dans les lieux publics. En cas de perte ou de vol, chaque utilisateur doit en rendre compte le plus rapidement possible selon la procédure en vigueur et transmettre la déclaration de vol faite auprès des services de police à la DOSI.

Verrouillage des équipements mobiles
Le verrouillage des équipements mobiles doivent être fait dés lors que l'on laisse les équipements sans surveillance. Par précaution, le verrouillage automatique doit être configuré pour ces équipements (réauthentification pour les portables et code à 4 chiffres de verrouillage de session pour les équipements de type Smartphone).

Parefeu des postes de travail nomades
Le parefeu des équipements nomades doit être configuré et activé dés lors qu'ils sont utilisés hors réseau Fnac Darty, afin de contrôler et gérer les flux entrants sortants sur ces domaines.

Connexion des équipements personnels au réseau Interne Fnac Darty
Les équipements personnels ne doivent en aucun cas être connectés au réseau informatique de Fnac Darty sans autorisation du sercice informatique.

Connexion des équipements Fnac Darty en mobilité
Les équipements Fnac Darty en mobilité ne doivent en aucun cas être connectés à des réseaux publiques Internet. Seules les réseau connus et maitrisés (domicile , bureau , etc …) sont autorisés.

Fiche n°15 . GESTION DES MENACES ET DES VULNERABILITES

Définition

Il s'agit d'un ensemble de mesures visant à protéger le SI Fnac Darty contre les tentatives d'intrusion et attaques basées sur l'introduction de code malicieux dans les composants informatiques (virus, bombe logique, chevaux de Troie, vers, etc…).

Risques

- Indisponibilité de tout ou partie du système d'information Fnac Darty
- Destruction ou corruption de tout ou partie des données et des logiciels
- Engagement de la responsabilité de Fnac Darty dans la contamination d'un correspondant.
- Surveillance et captation illicite de données du patrimoine Fnac Darty

Exigences

Antivirus
S'assurer que tous les mécanismes antivirus (moteur et signatures) sont adaptés quant à l'environnement à protéger, mis à jour automatiquement et en cours d'exécution avec des analyses définies à intervalles réguliers.

Déploiement des patchs de sécurité
Tous les correctifs de sécurité fournis par les éditeurs de systèmes d'exploitation et de logiciels de base doivent être validés par la DOSI, puis testés, qualifiés puis déployés sur les serveurs et postes de travail en fonction du risque identifié pour définir la priorité des correctifs à installer.

Suivi d'obsolescence de version
Les composants logiciels doivent faire l'objet d'un suivi d'obsolescence de version sous l'angle sécurité. Pour toute version de logiciel pour laquelle il est identifié que la délivrance des correctifs de sécurité ne sera plus assurée par le fournisseur, un plan d'actions de migration ou de suppression doit être défini. Ce point sera intégré dans l'analyse de risques.

Fiche n°16 . REGLES D'EXPLOITATION

Définition

Il s'agit d'un ensemble de mesures d'exploitation visant à sécuriser le SI

Risques

- Non prise en compte des exigences de sécurité.
- Dysfonctionnement par méconnaissance des mesures de sécurité

Exigences

Gestion des changements
Il convient de planifier les changements, à en apprécier les risques et à prévoir les procédures de mise en œuvre. Il est nécessaire de prévoir des retours en arrière en cas de problème, de vérifier que tous les acteurs impliqués sont informés et que les différents responsables ont donné leur accord pour le changement.

Dimensionnement du système
Des mesures doivent être prises pour garantir la capacité de traitement du SI. Il faut également vérifier que les nouveaux dispositifs ne vont pas consommer trop de ressources et surveiller la charge du système et de supprimer les équipements et les données devenues inutiles.

Isolation des environnements de développement et de production
Il est nécessaire de séparer les environnements (matériels, logiciels) de développement informatique (développement, maintenance, test, intégration) et de production.

Journalisation des événements
Il est nécessaire de journaliser les événements jugés les plus pertinents et en particulier l'activité des administrateurs.

Anonymisation des données de test
Il est nécessaire de rendre les données sensibles anonymes avant de les utiliser à des fins de test ou de développement.

Fiche n°17 . EXPLOITANTS DE LA DOSI

Définition

Les administrateurs, développeurs, exploitants au sens large du Système d'Information sont amenés à être dotés de droits d'accès privilégiés sur certaines ressources. Aussi il convient de fixer les règles de déontologie qu'ils s'engagent à respecter.

Risques

- Détournements des règles de sécurité
- Surveillance et captation illicite de données du patrimoine Fnac Darty

Exigences

Devoir de confidentialité des exploitants
Tous exploitants DOSI sont soumis à une obligation de discrétion liée à leurs activités. Ils respectent la confidentialité des informations auxquelles ils ont accès en particulier : les données à caractère personnel contenues dans le système d'information, les fichiers utilisateurs, les flux sur les réseaux, ¬ les courriers électroniques, ¬ les mots de passe, les traces des activités des utilisateurs , etc … Ils ne se connectent pas et ne donnent pas accès à des ressources sans y avoir été autorisés.

Sécurisation de leur périmètre
Tous exploitants DOSI doivent mettre en œuvre toutes les mesures de sécurité attendues dans la présente PSSI dans la limite des moyens dont il dispose. En particulier, ils sont responsables de la qualité des mots de passe de leur compte d'accès à fort privilège et des comptes de service qu'ils mettent en place. Des mots de passe faibles ,triviaux ou par défaut constituent une faille de sécurité , exploitée largement par les hackers.

Prise de contrôle à distance
La prise de contrôle à distance d'une session utilisateur à des fins de support doit au préalable obtenir son consentement. L'utilisateur doit conserver la visibilité sur les actions réalisées sur son poste et doit avoir la possibilité d'interrompre à tout moment la prise de contrôle à distance.

Privilèges accordés au mainteneur ou au télé-mainteneur
Les privilèges accordés au mainteneur ou au télé-mainteneur doivent être strictement limités à ceux nécessaires pour l'exercice de sa mission.

Fiche n°18 . DEVELOPPEMENT APPLICATIF

Définition

Il s'agit de définir les directives de sécurité s'appliquant lors de tout développement applicatif par les Directions de la DOSI.

Risques

- Non prise en compte des exigences de sécurité dans le développement applicatif.
- Dysfonctionnement par méconnaissance des exigences de sécurité

Exigences

Intégrer la sécurité au cœur des développements dans une démarche Sécurité par design
Par sécurité par design on entend la sécurité directement intégrée dans le code source de son application, de son site web, etc… Le but étant de réduire la surface d'attaque dès le code, ne pas laisser de failles, ou autoriser un accès interdit. Tout développement ou modification de code doit donner lieu avant sa mise en exploitation à l'exécution de procédures de recettes unitaires, d'intégration et de qualification afin de s'assurer que les bonnes pratiques de programmation en vigueur sont appliquées.

Sécurité dans les projet IT
Tout nouveau développement d'application doit respecter les obligations réglementaires et contractuelles imposables à Fnac Darty ainsi que la stratégie de sécurité définie par l'entreprise. Il est donc nécessaire d'intégrer la sécurité dans la gestion de projet afin d'apprécier les risques puis d'intégrer des points de sécurité à tous. Pour se faire, il doit être défini au préalable par le métier. ❑ Les critères de disponibilité de l'application (ceux-ci auront un impact sur la sauvegarde des données, la solution de redondance des systèmes ainsi que la définition d'un mode dégradé) ❑ Les critères de confidentialité (authentification, politique d'attribution, chiffrement des données , cloisonnement des données, falsification des données) ❑ Les critères de traçabilité (logs d'accès, logs applicatifs obligatoires pour les données personnelles par exemple) ❑ Intégrer les processus de développement en vigueur au sein de Fnac Darty,

Formats de données nécessaires pour la mise en production
S'assurer que les formats de données soient compatibles avec ❑ la mise en œuvre d'une durée de conservation et de purge ❑ le contrôle d'accès aux données ❑ la traçabilité via les journaux d'audits

Fiche n°19 . RELATIONS AVEC LES FOURNISSEURS

Définition

Il s'agit de définir la protection des actifs de l'organisation accessibles aux prestataires afin de maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux accords conclus avec les prestataires.

Risques

- Non prise en compte des exigences de sécurité.
- Dysfonctionnement par méconnaissance des exigences de sécurité

Exigences

Sécurité dans les accords conclus avec les pretataires
Les exigences de sécurité sont précisées dans les documents de consultations et contractuelles.

Surveillance et revue des services des prestataires
Le service informatique surveille, revoit à intervalles réguliers les prestations des services assurés par les prestataires de la DOSI. En cas d'écart, les indicateurs de performance prévus au contrat font l'objet de plan d'action de remédiation.

Fiche n°20 . GESTION DES INCIDENTS DE SECURITE

Définition

La supervision et la gestion de la sécurité doit permettre à Fnac Darty de détecter, de réagir et de traiter les incidents de sécurité qui sont des actes malveillants contre le SI (attaques virales, tentatives d'intrusion, captation de données …etc). La supervision doit être la plus proactive possible pour détecter et stopper au plus vite toutes actions malveillantes. L'ensemble des incidents de sécurité doit faire l'objet d'un tableau de bord.

Risques

- Non détection de tentative d'intrusion.
- Non détection d'utilisation anormale d'un accès au système d'information.
- Impossibilité d'analyser les causes d'un incident de sécurité.

Exigences

Traitement des incidents de sécurité et Escalade
Un incident de sécurité doit être signalé à la DOSI dès sa découverte, pris en charge et traité en priorité, pour en minimiser les conséquences et les impacts sur le SI de Fnac Darty. L'ensemble des incidents de sécurité doit faire l'objet d'un tableau de bord émis par la Direction Production et à destination du RSSI. Tout incident de sécurité à criticité élevée des systèmes d'information doit être systématiquement communiqué à la Direction Prévention des risques ainsi qu'aux SI des filiales et Pays.

Détection et prévention d'intrusion
L'ensemble des composants informatiques du SI de Fnac Darty doit faire l'objet d'une surveillance pour - détecter la survenance de tout incident de sécurité et notamment des attaques virales, des tentatives d'intrusion ou des utilisations frauduleuses, - tenter d'identifier les causes et les origines, - éviter des contaminations d'autres sites par rebond et de remettre en place le système. Pour se faire, le SI comprend des dispositifs, notamment : - de journalisation, - de filtrage et analyse des communications réseaux (parfefeu) - de systèmes de détection et prévention d'intrusion (IDS/IPS) - d'une console anti-virus couvrant le périmètre de Fnac Darty.

Contrôle de conformité des mesures de Sécurité selon le CSD IBM
Chaque semaine, un agent de contrôle de conformité de sécurité scanne les serveurs IBM et adresse au RSSI toutes les déviations relevées contraires au document de référence CSD.

Tirer les enseignements des incidents
Afin d'améliorer le processus de gestion des incidents il est recommandé d'organiser des retours d'expérience pour comprendre les causes des incidents

Recueil des preuves
Il est très important de collecter des preuves de façon fiable en cas de poursuites judiciaires.

Fiche n°21 . AUDITS DE SECURITE

Définition

L'audit a pour objectif de contrôler :

- la conformité des mesures mises en œuvre avec les exigences de sécurité en vigueur,
- la conformité des exigences de sécurité en vigueur par rapport aux enjeux de l'entreprise.

Risques

- Non conformité des mesures mises en œuvre par rapport aux exigences de sécurité exprimées.
- Perte de conscience des acteurs organisationnels et fonctionnels et des utilisateurs à la problématique sécurité.

Exigences

Audits de Sécurité
Des audits de sécurité du SI doivent être planifiés et réalisés périodiquement sous la direction de la DSSI afin d'évaluer l'adéquation des mesures de sécurité mises en œuvre, compte tenu des exigences réglementaires et contractuelles de sécurité en vigueur et des objectifs de sécurité de. Un Plan annuel d'audits de sécurité doit être établi.

SECURITE DES COMMUNICATIONS

Fiche n°22 . SECURITE DU RESEAU FNAC DARTY

Définition

La sécurité des réseaux locaux et inter sites s'exprime en terme d'accessibilité, de disponibilité et de confidentialité des données du réseau Fnac Darty.

Risques

- DENI de service
- Prise de contrôle non autorisée à des fins malveillantes des composants actifs du réseau
- Ecoute non autorisée à des fins malveillantes des flux de données.

Exigences

Disponibilité du réseau
Les éléments actifs principaux des différents réseaux locaux de Fnac Darty doivent être redondés pour permettre une continuité de fonctionnement en cas d'incident matériel.

Maîtrise de l'architecture réseau
L'architecture du réseau interne de Fnac Darty et des points d'interconnexion avec les réseaux externes doit être maitrisée, documentée et tenue à jour par la DOSI. Toute évolution en terme d'architecture réseau et d'interconnexions doit être soumise à la Direction de la Sécurité de SI afin de veiller à bien prendre en compte les risques en termes de Sécurité du SI.

Sécurisation des zones externes, internes
Exigence d'un pare-feu au niveau de chaque connexion Internet, de toute zone démilitarisée (DMZ) et la zone de réseau interne, avec contrôle des règles des pare-feu et routeurs au moins tous les six mois.

Segmentation et protection des ressources
Les réseaux locaux et étendus de doivent être segmentés afin de permettre un cloisonnement logique, spécifique aux ressources sensibles, notamment entre les sites géographiques, les flux métiers, les profils utilisateurs. Les segmentations logiques, physiques, filaires ou avec wifi doivent être documentées, mises à jour par la DOSI. Toute évolution doit être soumise au RSSI afin de veiller à bien prendre en compte les risques en termes de Sécurité du SI.

Cloisonnement de la Téléphonie sur ip
Un contrôle de flux adapté aux protocoles utilisés doit être mis en œuvre afin de segmenter et cloisonner la téléphonie sur ip en ne laissant passer que les flux autorisés.

Cloisonnement des environnements avec données sensibles
Le trafic entrant et sortant doit être restreint au trafic strictement nécessaire à l'environnement des données sensibles de l'entreprise et conformément à la réglementation en vigueur.

Confidentialité du réseau Wifi
De part l'accessibilité du signal, les réseaux WIFI sont particulièrement exposés à des tentatives d'intrusion. Dans ce cadre, le point d'accès doit être configuré afin d'utiliser : ✓ Un chiffrement robuste (au minimum WPA2) ✓ Une confidentialité maximum (SSID masqué) ✓ Un déploiement automatique des informations de connexion au WIFI (nom du réseau, clé d'accès, certificats éventuels, etc) par GPO ou autre dispositif, afin de ne pas les communiquer aux utilisateurs. Toutes déviations à ces règles de sécurité doivent être déclarées auprès du RSSI et revues annuellement lors de la mise à jour des Directives Techniques des mesures de contrôles.

Fiche n°23 . SECURITE DES ACCES AU RESEAU

Définition

La sécurité des accès concerne

- les accès des utilisateurs au système d'information Fnac Darty
- les accès entrants des utilisateurs du système d'information Fnac Darty à partir d'un poste distant Fnac Darty ou non maîtrisé par la DOSI, via une liaison sécurisée de type VPN SSL.
- La mise en œuvre d'une interconnexion avec un réseau externe partenaire.
- Les flux d'échange via une plateforme EDI

Risques

- DENI de service
- Intrusion depuis le monde extérieur dans le SI de Fnac Darty pouvant entraîner un détournement de données stratégiques, une corruption des données ou leur destruction.
- Contamination du SI par des codes malicieux (virus, chevaux de Troie, ver).

Exigences

Contrôle d'accès au réseau Fnac Darty
L'accès aux réseaux locaux et étendus de Fnac Darty est limité aux seules personnes autorisées par la DOSI, après une authentification nominative au niveau du poste de travail et/ou du serveur.

Interconnexion avec un réseau externe
Chaque point d'interconnexion avec un réseau externe doit être maintenu et supervisé du point de vue de la sécurité afin de ne laisser passer que les seuls flux autorisés.La mise en œuvre d'une interconnexion avec un réseau externe doit se faire uniquement à travers une solution autorisée et soumise au préalable de sa mise en œuvre à la Direction de la Sécurité des SI afin de s'assurer que toutes les exigences de sécurité vont être respectées.

Accès VPN utilisateur
Chaque compte d'accès Vpn doit être soumis à validation du supérieur hierarchique de l'utilisateur.

Accès partenaire
Les accès Vpn SSL sont interdits. Seuls les accès Vpn Ipsec sont autorisés . L'accès du partenaire doit être limités dans le temps et ne permettre l'accès qu'aux ressources informatiques liées à sa mission. Il est assujetti au changement régulier de mot de passe.

Fiche n°24 . UTILISATION DES OUTILS DE COMMUNICATION

Définition

Il s'agit de définir les exigences liées à l'utilisation des moyens électroniques de communication (messagerie, Internet, téléphone, les forums de discussion, etc. …) mis à la disposition des salariés et des prestataires externes Fnac Darty, afin de garantir la sécurité du système d'information et éviter les abus.

Risques

- Diffusion d'information confidentielle à l'extérieur de l'entreprise
- Saturation ou indisponibilité des moyens électroniques de communication
- Diffusion de messages pouvant nuire à l'image de la société ou d'un employé

Exigences

Messagerie professionnelle
Les moyens électroniques de communication fournis par Fnac Darty sont à usage professionnel. Les messages personnels envoyés par l'utilisateur doivent expressément en porter la mention « PRIVEE » dans leur objet, et être stockés dans un dossier créé à cet effet, afin d'exprimer sans ambigüité le caractère extra-professionnel du message.

Utilisation de l'adresse interne Fnac Darty
Aucun utilisateur ne doit communiquer ses coordonnées, en particulier son adresse électronique, sur des sites sans rapport avec son activité professionnelle ou dont l'image est incompatible avec celle de Fnac Darty. Par ailleurs, la publication d'adresses électroniques professionnelles sur des sites publics expose les utilisateurs à recevoir des emails non sollicités (phénomène du spamming).

Echanges de données confidentielles
Les utilisateurs doivent chiffrer le fichier contenant des données personnelles au préalable d'un envoi via messagerie avec la solution ZIP de la DOSI mise à leur disposition sur leur poste de travail ou utiliser la solution de stockage en ligne mise en place par la DOSI .

Echanges de données volumineuses
Pour les données trop volumineuses, les utilisateurs doivent utiliser la solution de stockage en ligne mise en place par la DOSI.

Usage illicite des services publics de stockage en ligne

En aucun cas, l'utilisateur ne stocke des données du SI sur des supports non Fnac Darty, ni n'utilise des solutions grand public de type Dropbox, Skydrive, Google Docs où la sécurité et la confidentialité des données stockées dans le Cloud ne sont pas garanties. Seule la solution mis en œuvre par la DOSI est autorisée.

Plateforme EDI

Tous les échanges réguliers de fichiers avec les fournisseurs et partenaires de Fnac Darty doivent passer par le flux supporté par la plate-forme EDI.

Comportement face à un message non sollicité

Chaque utilisateur doit faire preuve de vigilance à l'égard des messages indésirables (spam) et douteux (canulars, phishing …). L'utilisateur recevant ces messages ne doit donc en aucun cas y répondre, les transférer ou les imprimer, et doit s'assurer de leur destruction immédiate. En cas de doute, se rapporcher de l'équipe Sécurité de la DOSI.

Fonctions de redirection automatique

Aucun utilisateur ne doit mettre en œuvre des fonctions d'envoi ou de redirection automatique de messages vers une adresse de messagerie hors du domaine Fnac Darty.

Usage responsable et modéré des outils de communication

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et strictement nécessaire à l'activité professionnelle, sous réserve d'une utilité au regard des fonctions et missions de l'utilisateur.

L'usage d'Internet doit être modéré, ceci afin de ne pas saturer le service global INTERNET, mis à disposition par Fnac Darty. Il évitera les usages Internet liés à la vidéo (téléchargement et lecture video via streaming notamment Youtube) ainsi qu'au son (radio via internet, service de streaming audio).

En cas de nécessité pour le travail, les téléchargements ''lourds'' (applicatifs , OS , etc…) doivent être fait dans des plages horaires où l'activité est au plus bas, et toujours en concertation avec la DOSI.

La consultation d'un site pour motifs personnels, ne mettant pas en cause les intérêts et la réputation de Fnac Darty, est tolérée à condition de ne pas affecter le travail de l'utilisateur, tant d'un point de vue quantitatif que qualitatif, ni l'accomplissement de ses missions, ni la sécurité de son poste et plus généralement la sécurité du Système d'Information.

CONTINUITE DES ACTIVITES DU SI

FICHE N°25 . POLITIQUE DE SAUVEGARDE & ARCHIVAGE
FICHE N°26 . PLAN DE REPRISE D'ACTIVITE

Fiche n°25 . POLITIQUE DE SAUVEGARDE & ARCHIVAGE

Définition

Il s'agit d'un ensemble de mesures visant à être en capacité de restaurer des données suite à la détérioration ou altération des données du SI.

Risques

- Indisponibilité de tout ou partie du système d'information Fnac Darty
- Destruction ou corruption de tout ou partie des données et des logiciels

Exigences

Sauvegarde
Pour chaque environnement de production, la sauvegarde applicative (code source) et des données doit être définie et mise en œuvre. Annuellement, des tests de restauration doivent être réalisés pour valider l'intégrité et la capacité à redémarrer sur un autre environnement. Certaines sauvegardes peuvent être archivées.

Conservation des sauvegardes et archives
Leur stockage doit être sécurisé ce qui implique : ✓ une limitation et gestion des accès logiques et physiques, ✓ un espace de stockage différent des espaces de production physique et logique. Les durées de conservation et de purge réglementaires sont respectées et notamment dans le cadre des données personnelles.

Fiche n°26 . PLAN DE REPRISE D'ACTIVITE

Définition

Il s'agit d'un ensemble de mesures visant à la coordination et la mise en œuvre du plan de reprise d'activité informatique (PRAI) définie en cas de survenance d'un incident majeur entraînant une indisponibilité partielle ou totale du SI.

Risques

- Incapacité de reprendre tout ou partie de l'activité Fnac Darty en cas de réalisation d'un incident ou d'un sinistre, dans un délai conforme aux besoins métiers de l'entreprise
- Arrêt du business

Exigences

Classification des applications et services par criticité
Chaque application est gérée en fonction de sa criticité. Cela implique la définition des niveaux de service attendus SLA (par exemple GOLD, ARGENT et BRONZE pour les applications infogérées chez IBM)

Ordre de démarrage lors d'une reprise d'activité SI
La Direction Production des SI définit les conditions de redémarrage et notamment l'ordre de démarrage auprès de l'infogéreur en cas d'incident majeur. Cet ordre est revu annuellement.

Plateforme de secours SI
Chaque Datacenter de Fnac Darty doit être en capacité de redémarrer partiellement dans une plateforme de secours déportée suite à l'indisponibilité physique ou logique, totale ou partielle du Datacenter.

Test du Plan de reprise d'activité SI
Il convient d'établir un plan de contrôle régulier prévoyant la périodicité et la nature des tests à effectuer afin d'en identifier les manquements et établir un plan d'action de remédiation. La fiabilité des sauvegardes des données et des codes sources applicatifs ainsi que l'ordonnancement des relances applicatives avec les durées imparties, doivent être revues annuellement.

Plan de Management de crise informatique
Il convient d'établir un plan de management de gestion de crise informatique (PMCI), définissant les modalités de mobilisation et de composition de la cellule de crise ainsi que l'ensemble des premières mesures en termes de communication. Le PMCI intègre le plan de Gestion de crise Global de Fnac Darty, piloté par la Direction Prévention des risques de Fnac Darty.

CONFORMITE

FICHE N°27 . DROIT INTERNET - LUTTE CONTRE LA CYBERCRIMINALITE
FICHE N°28 . DROITS DE PROPRIETE INTELLECTUELLE
FICHE N°29 . PROTECTION DE LA VIE PRIVEE ET DES DONNEES PERSONNELLES
FICHE N°30 . PCI DSS

Fiche n°27 . DROIT INTERNET - LUTTE CONTRE LA CYBERCRIMINALITE

Définition

La loi française pour la Confiance dans l'Économie Numérique (LCEN) du 22 juin 2004 comprend 58 articles ayant pour vocation de poser les fondations du droit de l'Internet.

Cette loi traite de la responsabilité et des obligations des « prestataires techniques » de services Internet (hébergeurs de sites, entreprises fournissant un accès Internet entreprise, acteurs du commerce électronique), notamment :

- **Devoir de dénonciation de toutes activités répréhensibles** (crimes contre l'humanité, incitation à la haine raciale, pornographie enfantine, etc) qui serait exercée au travers des services qu'ils rendent.
- **Obligation d'information** à leurs utilisateurs de l'existence de moyens techniques de contrôles et de restriction à certains services Internet.
- **Obligation de conservation** des données de nature à permettre l'identification de quiconque a contribué à la création du contenu mis en ligne soit les logs de connexions et d'authentification. La durée de conservation est définie à 1 an par décret d'État du 25 février 2011.

Risques

- Non-conformité
- Sanctions pénales
- Atteinte à l'image de marque.

Exigences

Accès Internet et activités illégales
L'utilisation d'Internet, de la messagerie électronique et des moyens informatiques au sens large (messagerie instantanée, listes d'informations, etc.), de manière illégale par le personnel de Fnac Darty peut conduire la direction à être responsable des illégalités constatées. Par conséquent, une sensibilisation des utilisateurs ainsi que des mesures de contrôle et de restriction des accès Internet doivent être mises en œuvre : ✓ Interdiction de consulter des sites illégaux (pédophilie, racisme, xénophobie, etc.), ✓ Interdiction de diffuser des informations à caractère raciste, diffamatoire, etc., ✓ Interdiction d'utiliser les ressources du Système d'Information pour exercer des pratiques illégales (prêt d'argent en ligne, contrefaçon, recel, etc.).

Conservation des logs de connexion internet
La journalisation des logs Internet doit permettre l'identification de quiconque a contribué à la création du contenu mis en ligne soit les logs de connexions et d'authentification. La durée de conservation est définie à 1 an par décret d'État du 25 février 2011.

Fiche n°28 . DROITS DE PROPRIETE INTELLECTUELLE

Définition

Il s'agit pour Fnac Darty de respecter les dispositions du code de la propriété intellectuelle relatives à la propriété littéraire et artistique (logiciels et œuvres de l'esprit d'une manière générale), aux marques, aux dessins et modèles.

Les produits logiciels propriétaires sont généralement fournis sous contrat de licence qui limite l'utilisation de ces produits à des machines spécifiées ou en limite parfois la copie à la création de copies de sauvegarde uniquement. De même, certains documents (au format papier ou électronique) sont protégés par des droits d'auteur. Le non-respect de la législation sur les droits de propriété intellectuelle peut entraîner des actions en justice à l'encontre de Fnac Darty et de ses employés

Risques

- Non-conformité
- Sanctions civiles et pénales
- Atteinte à l'image de marque.

Exigences

Propriété intellectuelle
Il convient d'appliquer des procédures appropriées afin de veiller au respect des obligations liées au code de la protection intellectuelle pour les acquisitions de licences logicielles. Une revue annuelle est menée pour évaluer notre niveau de conformité en terme de licences . Entre autre, il convient de considérer les mesures suivantes : ✓ La conservation de preuves d'achat et de propriété de licences, de disques d'exploitation, de manuels, etc., ✓ La mise en œuvre de contrôles pour faire en sorte que le nombre maximum d'utilisateurs permis ne soit pas dépassé et que seuls les logiciels autorisés et les produits fournis sous licence soient installés sur les postes de travail et les serveurs de Fnac Darty, ✓ L'établissement de procédures d'acquisition, de mise hors service ou de transfert à d'autres entités de produits logiciels, ✓ Le respect des modalités et des conditions relatives aux logiciels et aux informations obtenues via des réseaux publics, ✓ L'information du personnel sur les problématiques juridiques associées aux droits sur la propriété intellectuelle au moyen de procédures opérationnelles, de chartes ou de documents de sensibilisation, ✓ Etc.

Fiche n°29 . PROTECTION DE LA VIE PRIVEE ET DES DONNEES PERSONNELLES

Définition

Le règlement n° 2016/679, dit règlement général sur la protection des données (RGPD ou GDPR en anglais), constitue le texte de référence en matière de protection des données à caractère personnel, applicable à compter du 25 mai 2018. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

Les données personnelles sont les informations qui permettent d'identifier directement ou indirectement une personne physique. Elles correspondent aux noms, prénoms, adresses , IP, numéro de téléphone, lieu et date de naissance, numéro de carte de paiement, photo, cookies de navigation, etc.

Tout responsable de traitement informatique de données personnelles, soit le responsable applicatif des données personnelles doit veiller à :

- Définir et adopter les mesures de sécurité adaptées à la nature des données et aux risques présentés par le traitement,
- S'assurer de la confidentialité des données et notamment des habilitations des personnes autorisées à accéder aux données personnelles applicatives,
- Permettre aux personnes dont il détient des informations, d'exercer pleinement leurs droits,
- Définir une durée de conservation des données personnelles pour des raisons opérationnels ou juridique ainsi que d'effacement/destruction lorsque celles-ci sont obsolètes ou ne sont plus nécessaires à l'activité du groupe.

Risques

- Non-conformité
- Sanctions pénales

Exigences

Revue annuelle de conformité CNIL
Une revue annuelle doit mesurer le niveau de conformité de Fnac Darty et notamment le respect des durées de conservation (archive courante – intermédiaire – purge) conformément aux déclarations CNIL sur les données personnelles collectées ainsi que les conditions de traitement du droit d'accès, de rectification, de suppression et d'opposition sur ces données personnelles.

Respect de la législation sur le traitement des données personnelles

Fnac Darty doit respecter les obligations relatives au traitement de données à caractère personnel édictées par la CNIL et traitant des sujets suivants :

- ✓ Collecte de données personnelles (autorisation de l'intéressé, exactitude des données, ne collecter que ce qui est strictement nécessaie , etc.),
- ✓ Finalité des traitements opérés (objectif précis et exploitation cohérente),
- ✓ Durée de conservation des informations,
- ✓ Protection des données (mesures de sécurité physiques et logiques),
- ✓ Droit d'accès , droits d'opposition, de modification et de suppression des données personnelles,
- ❑ Confidentialité des données (seules les personnes autorisées peuvent accéder aux données personnelles)
- ❑ Tracabilité des accès aux données
- ❑ Notifications des violations de données personnelles

Les développements informatiques autour de la donnée personnelle

La protection des données à caractère personnel doit être partie intégrante du développement informatique afin d'empêcher toute erreur, perte, modification non autorisée, ou tout mauvais usage de celles-ci dans les applications.

Les précautions élémentaires sont les suivantes :

- ❑ Les applications en développement et celles en opération fonctionnent sous différents systèmes et dans différents domaines ou répertoires
- ❑ Les utilisateurs ont des profils distincts pour les systèmes opérationnels et ceux de tests ;
- ❑ Les données sensibles ne sont pas importées ou copiées sans anonymisation dans le système de test ;
- ❑ Les systèmes de développement et de test n'ont pas accès à l'environnement de production.

Processus de validation de la conformité des projets

Tout nouveau projet impliquant un traitement de données personnelles avec un partenaire doit donner lieu à une documentation, validation de l' équipe DPO et RSSI ainsi qu'une sécurisation contractuelle.

Extractions des données personnelles

Toute manipulation , toute extraction ou tout transfert de données personnelles est interdit sans validation du DPO. Les données personnelles doivent être anonymisés autant que possible et des mesures de sécurité garantissant la sécurité et la confidentialité de ces données doivent être prévues.

Confidentialité, Authentification et Traçabilité des accès aux données personnelles

La CNIL demande que les accès aux données soient limités au stricte nécessaire et tracés. Cela implique

- Une gestion des habilitations et des comptes
- Un login personnel avec un mot de passe complexe de 10 caractères minimum
- La conservation pendant 6 mois maximum des logs de connexions (accès à l'application) ainsi que les traces applicatives (accès aux données en lecture , écriture , modification, suppression).

Procèdure de violationde donnée

Une procédure de notification de violation des données doit être rédigée, tant chez les responsables de traitement que les sous-traitants, intégrant les étapes clés suivantes :

- Prévoir un système interne de signalement
- Prévoir une investigation
- Prévoir la mise en oeuvre de mesures correctives
- Notifier à la cnil s'il ya eu compromission

Politique de délais de conservation

Une politique de conservation à caractère personnel a été définie pour le groupe. Elle est diffusée et accessible à l'ensemble des collaborateurs de Fnac darty, pouvant avoir accès, ayant accès, ayant eu accès ou étant amenés à voir accès à des documents ou des Données Personnelles au sein de Fnac Darty, et qui doivent la respecter.

Elle a pour but de décrire et formaliser les opérations nécessaires au sein du groupe afin d'assurer :

- La conservation et la destruction des documents,
- La conservation et l'effacement des données personnelles, au sens des dispositions légales et règlementaires applicables.

Fiche n°30 . PCI DSS

Définition

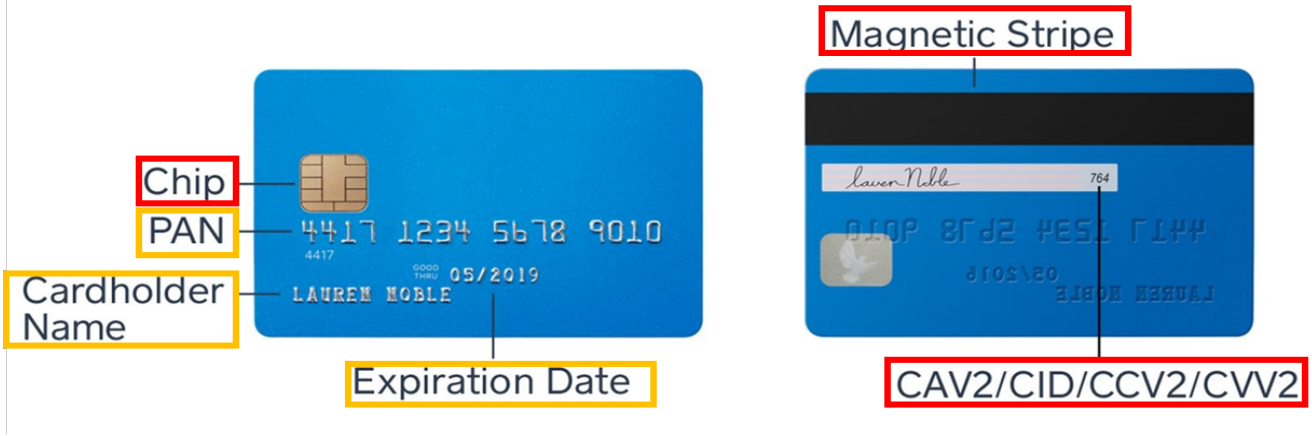
Le programme PCI DSS (Payment Card Industry Data Security Standard) est une norme contractuelle (Visa, MasterCard) de sécurité établie pour garantir le traitement, la transmission et le stockage des données des titulaires de cartes de manière sécurisée.
Il s'applique aux marchands et autres prestataires de services de paiement à partir du moment où ils traitent des numéros de carte (et donc même sans les stocker). Il définit des règles d'exigence en matière de sécurité que commerçants et/ou prestataires doivent respecter.

Risques

- Non-conformité
- Interdiction de traiter des cartes bancaires

Exigences

Les données cartes soumises à la norme PCI DSS



Il existe 2 types de données carte (card data):

- **Données d'identification carte du porteur / Cardholder data (CHD)** : Numéro de carte de paiement / PAN (Primary Account Number) + Nom du porteur de carte /Cardholder name + Date d'expiration /Expiration date.
  Les données cartes du porteur (**CHD**) peuvent être conservées si elles sont rendues illisibles par chiffrement.

- **Données sensibles d'authentification/ Sensitive authentication data (SAD)** : Données puce / Chip data + Données bande magnétique / Magnetic stripe data + Codes de vérification / CVV2.
  Les données sensibles d'authentification (**SAD**) ne doivent pas être conservées après autorisation, même chiffrées ;

Fnac Darty a une stratégie de se reposer sur des prestataires de confiance, spécialisés dans le stockage des PAN, afin de ne pas stocker cette information sur ses systèmes d'information.

12 règles de conformité PCI DSS
1. Installer et gérer une configuration de pare-feu pour protéger les données des titulaires de cartes 2. Ne pas utiliser les mots de passe système et autres paramètres de sécurité par défaut définis par le fournisseur 3. Protéger les données des titulaires de cartes stockées (chiffrement) 4. Chiffrer la transmission des données des titulaires de cartes sur les réseaux publics ouverts 5. Utiliser des logiciels antivirus et les mettre à jour régulièrement 6. Développer et gérer des systèmes et des applications sécurisées 7. Restreindre l'accès aux données des titulaires de cartes et aux seuls individus qui doivent les connaître (accès réseau) 8. Affecter un ID unique à chaque utilisateur d'ordinateur 9. Restreindre l'accès physique aux données des titulaires de cartes (accès physique) 10. Effectuer le suivi et surveiller tous les accès aux ressources réseau et aux données des titulaires de cartes 11. Tester régulièrement les processus et les systèmes de sécurité 12. Gérer une politique de sécurité des informations