XNATIS

Gestion

Comprendre la gestion des risques

XWNATIS

Compétence demandée :

Comprendre la gestion des risques

XMNATIS

1. Le dommage
2. Types de risques
3. Méthodologie
4. Les organisations
5. Les normes

XWIKI SAS

XWIKI NATIS

LE DOMMAGE

XWIKI NATIS

Qu‘est-ce qu‘un dommage ?

XONATIS

Un dommage est un dégât matériel ou immatériel, à une chose ou une personne

XWIKI NATIS

A partir de quel moment un dommage est grave ?

XWIKI SAS

XWIKI NATIS

La gravité est l’ampleur des dommages potentiels

La probabilité d’occurence est la probabilité de subir un dommage

XWIKI NATIS

La gravité est l’ampleur des dommages potentiels

La probabilité d’occurence est la probabilité de subir un dommage

XONATIS

XWIKI NATIS

La criticité est une mesure du risque :

criticité = probabilité d’occurence x gravité

XONATIS

XWIKI NATIS

TYPES DE RISQUES

XWIKI NATIS

Quels sont les types de risques ?

XWNATIS

Risque de réputation (image de l'entreprise)
Risque financier (perte ou maque à gagner)
Risque systémique (effet boule de neige)
Risque social (comportements)
Risque opérationnel (gestion de l'activité)
Risque légal (réglementaire)

XONATIS

Risque de réputation (image de l'entreprise)
Risque financier (perte ou maque à gagner)
Risque systémique (effet boule de neige)
Risque social (comportements)
Risque opérationnel (gestion de l'activité)
Risque légal (réglementaire)

XWIKI NATIS

Il n’y a pas de risque systématiquement plus grand car la criticité dépend de l’activité

XANATIS

Il n’y a pas de risque systématiquement plus grand car la criticité dépend de l’activité

XAINATIS

Risque de réputation (image de l'entreprise)
Risque financier (perte ou maque à gagner)
Risque systémique (effet boule de neige)
Risque social (comportements)
Risque opérationnel (gestion de l'activité)
Risque légal (réglementaire)

XWNATIS

Règlement UE 2016/679 du Parlement européen

Le RGPD (Règlement Général sur la Protection des Données) dicte les mesures à adopter pour la protection des données à caractère personnel (DCP) sur le territoire de l'Union Européenne

XWIKI NATIS

Règlement UE 2016/679 du Parlement européen

Le RGPD (Règlement Général sur la Protection des Données) dicte les mesures à adopter pour la protection des données à caractère personnel (DCP) sur le territoire de l'Union Européenne

XWIKI NATIS

DCP (PII) ?

XWIKI NATIS

Article 4 du RGPD et article 2 de loi informatique et libertés

Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement

XWNATIS

Article 4 du RGPD et article 2 de loi informatique et libertés

Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement

XWIKI SAS

XWIKI NATIS

METHODOLOGIE

XWIKI NATIS

Comment mettre en place une gestion des risques ?

XWIKI NATIS

1. Planifier la gestion des risques
2. Identifier les risques
3. Estimer les risques
4. Maitriser les risques
5. Surveiller les risques

XWIKI NATIS

1. Planifier la gestion des risques

Comment organiser et planifier la gestion des risques dans une entreprise ?
Prenons une dizaine de minutes pour se sensibiliser !

XWIKI NATIS

1. Planifier la gestion des risques

Définir les tâches à accomplir et établir les responsabilités :

- en matière de politique d'acceptation des risques (les critères)
- concernant toutes les taches nécessaires à la gestion des risques

XONATIS

XWIKI NATIS

2. Identifier les risques

Comment identifier les risques ? Quelles sont les pistes à suivre ?
Prenons une dizaine de minutes pour se sensibiliser !

XNATIS

2. Identifier les risques

Les personnes / l'environnement / les équipement impliqués
Les scénarios menant aux situations dangereuses
Les dommages potentiels

les risques déjà connus,
les bonnes pratiques (guides, normes, spécifications, réglementation)
les possibilités techniques et les limites qui sont associées

XONATIS

XWIKI NATIS

3. Estimer les risques

Doit-on estimer les risques ?
Prenons une dizaine de minutes pour se sensibiliser !

XWIKI NATIS

3. Estimer les risques

Il faut estimer, de manière quantitative :

- les probabilités d’occurence
- les gravités

XONATIS

XWIKI NATIS

4. Maitriser les risques

Comment maîtriser les risques ?
Prenons une dizaine de minutes pour se sensibiliser !

XWIKI NATIS

4. Maitriser les risques

L’idée est de définir des mesures de réduction des risques :

- Suppression totale du risque
- Mise en place d’une prévention
- Compensation du risque s’il n’est pas réduit (par exemple avec une assurance professionnelle)

XONATIS

XNATIS

5. Surveiller les risques

Quelle méthodologie pour surveiller les risques ?
Prenons une dizaine de minutes pour se sensibiliser !

XWIKI NATIS

5. Surveiller les risques

Choisir les indicateurs pour surveiller les risques connus et de détecter les risques émergents

La définition des indicateurs n’est jamais figée, elle évolue avec votre compréhension des risques

XWIKI SAS

XWIKI NATIS

LES ORGANISATIONS

XWIKI NATIS

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service français créé par décret en juillet 2009.

L'ANSSI apporte son expertise et son assistance technique pour la sécurité des opérateurs d'importance vitale (OIV).

XMNATIS

https://www.ssi.gouv.fr/

XWIKI NATIS

Open Web Application Security Project (OWASP) est une communauté en ligne travaillant sur la sécurité des applications Web.

OWASP est aujourd'hui reconnue dans le monde de la sécurité des systèmes d'information pour ses travaux et recommandations liées aux applications Web.

XWIKI NATIS

https://owasp.org/

XMNATIS

LE TOP 10 des menaces

XWIKI NATIS

https://owasp.org/www-project-top-ten/

XMCO NATIS

1. A1_2017 : Les applications WEB ne vérifie pas assez les inputs et peuvent laisser passer du code

Chaque input est un vecteur d‘injection de code

XMNATIS

2. A2_2017 : Les fonctions applicatives liées à l'authentification et à la gestion des sessions sont souvent mal implémentées

Tester intensément les fonctions liées à l‘authentification

XMNATIS

3. A3_2017 : De nombreuses applications WEB ne protègent pas correctement les données sensibles, telles que les données financières, les soins de santé et les informations personnelles (DCP).

Vérifier les risques de fuite de données (obligations légales)

XMNATIS

4. A4_2017 : Utilisation de technologies trop anciennes (XML processor) permettent d’exécuter du code externe et hostile.

Restez à jour dans les technologies utilisées ou alors pensez à bien les configurer

XWIKI NATIS

5. A5_2017 : Les restrictions sur ce que les utilisateurs authentifiés sont autorisés à faire ne sont souvent pas correctement appliquées

Tester le périmètre d'application des rôles

XWIKI NATIS

6. A6_2017 : La mauvaise configuration de la sécurité est le problème le plus fréquemment rencontré. Ceci est généralement le résultat de configurations par défaut non sécurisées ou de configurations incomplètes.

Ne pas laisser la configuration par défaut

XWIKI NATIS

7. A7_2017 : Cross-Site Scripting XSS affichage d’éléments HTML non contrôlés (comme les commentaires qui peuvent contenir des éléments HTML)

Bien contrôler les inputs

XWIKI NATIS

8. A8_2017 : Certains systèmes permettent une exécution de code à distance

Limiter le périmètre d'exécution de code et permettre uniquement l'exécution de code déjà présent sur le serveur

XWIKI NATIS

9. A9_2017 : Les composants, tels que les bibliothèques, les frameworks et autres modules logiciels, peuvent présenter des failles de sécurité

Ne faire confiance qu‘aux librairies, frameworks et modules qui sont populaires et bien testés

XWIKI NATIS

10. A10_2017 : Une surveillance insuffisante des systèmes permettent aux hackers d'attaquer davantage les systèmes informatiques

Surveiller de manière continuelle les comportements étranges des visiteurs (proposer par exemple des captcha)

XWIKI NATIS

LES NORMES

XWIKI NATIS

La norme ISO/CEI 27005 est une norme internationale concernant la Sécurité de l'information publiée conjointement par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) basé sur l’amélioration continue (PDCA)

XWIKI NATIS

La norme ISO 9001 est une norme internationale concernant le Système de Management de la Qualité (SMQ) publiée par l'Organisation internationale de normalisation (ISO).

Cette norme définit des exigences pour améliorer en permanence la satisfaction de leurs clients et fournir des produits et services conformes

XONATIS