XNATIS

Risques

Comprendre la gestion des risques

XWNATIS

Compétence demandée :
Comprendre la gestion des risques

XWNATIS

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

XWIKI SAS

XWIKI NATIS

LE DOMMAGE

XWIKI NATIS

Un dommage est un dégât matériel ou physique, 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

XWIKI SAS

XWIKI NATIS

La criticité est une mesure du risque :

criticité = probabilité d'occurence x gravité

XWIKI SAS

XDNATIS

TYPES DE RISQUES

XWIKI NATIS

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

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

XWIKI NATIS

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

XWIKI NATIS

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

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

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

XWIKI SAS

XWIKI NATIS

METHODOLOGIE

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

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

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

XWIKI NATIS

3. Estimer les risques

Il faut estimer, de manière quantitative :

- les probabilités d’occurence
- les gravités

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

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

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

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).

XWIKI SAS

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

XWIKI SAS