

Résumé

Ce document décrit ce qu'on entend par la sécurité physique, la différence entre des mesures préventives et des mesures protectrices, les spécificités des locaux informatiques ainsi que diverses recommandations ou règles de mise en place. Les conseils sont en général applicables dans tout environnement informatique, bien que certains concernent spécifiquement de grands centres de calculs. Les incidents ou menaces physiques potentiels sont les suivantes :

- > les dégâts des eaux,
- > les dégâts du feu,
- > les dégâts liés à l'électricité,
- > les défauts de climatisation,
- > les incidents de télécommunication,
- > les intrusions physiques,
- > les phénomènes électrostatiques,
- > l'inaccessibilité du centre informatique, avec une description des conséquences possibles, ainsi que des mesures de prévention et de protection applicables.

Table des matières

- 1 Qu'entend-on par la sécurité physique ? →
- 2 Qu'entend-on par les mesures préventives et protectrices ? →
- 3 Le local informatique, est-ce qu'il existe des différenciations ? →
- 4 Comment se protéger contre des incidents ? →



1 Qu'entend-on par la sécurité physique ?

La sécurité physique vise à favoriser l'exploitation des équipements informatiques dans des conditions fonctionnelles optimales de

manière à en retirer le maximum de performances durant la plus longue période possible.

2 Qu'entend-on par les mesures préventives et protectrices ?

Quand on parle de mesures ou parades, il faut faire la différence entre les actions préventives et les actions protectrices.

- Les mesures préventives ont pour but d'éviter qu'un sinistre ne survienne.
- Les mesures de protection ont pour but de protéger le patrimoine en cas de survenance du sinistre.

Il serait illusoire de penser que les mesures préventives rendent impossible tout sinistre. Même dans le cas de mise en place de ce type de parade, il est conseillé de déployer également des mesures de protection. L'ampleur des moyens de protection nécessaires est inversement proportionnelle aux moyens de prévention mis en place.

[→ suite](#)

3 Le local informatique, est-ce qu'il existe des différenciations?

Pour différentes raisons liées à la nature des équipements, à leurs conditions de fonctionnement, à leur criticité, au bruit ou à la chaleur dégagée, etc., il est judicieux de mettre en place des locaux informatiques dédiés, séparés des surfaces de travail utilisées par les employés.

On peut distinguer différents types de locaux informatiques, tels que :

3.1 Salle informatique de type «Data Center»

Cette salle héberge généralement tous les équipements spécialisés, nécessaires à la fourniture des ressources informatiques. On y trouve les serveurs, gros calculateurs, solutions de sauvegarde et de restauration des données, baies de stockage, etc..

Dans la plupart des sociétés de taille moyenne, cette salle contient également les éléments critiques du réseau (commutateurs, routeurs...) ainsi que les points d'accès et équipements servant à connecter la société vers le monde extérieur (central téléphonique, accès Internet...). Dans de plus grandes infrastructures, on trouve différentes salles spécialisées, appelées salle réseau, salle téléphonie et salle connectique.

Au niveau des très gros centres de calcul, on fait même la distinction entre la salle «morte» où se trouvent les équipements n'exigeant que très peu d'interventions humaines (processeurs, stockage...) et la salle «vive» où se trouvent les équipements nécessitant des interventions humaines fréquentes (robot de sauvegarde...).

3.5 Salle «connectique» d'étage

Au niveau des étages, on trouve habituellement des locaux servant à connecter les équipements de l'étage sur le tronc commun de câblage menant à la salle informatique. Ces salles contiennent ordinairement des panneaux de brassage ainsi que des commutateurs d'étage. Ces locaux et la connectique sont normalement conçus avec une redondance maximale, de manière à prévenir au maximum des ruptures éventuelles.

Etant donné la criticité de ces équipements, ces locaux sont considérés comme des locaux informatiques et sont donc soumis aux mêmes exigences de conception et de surveillance.

4 Comment se protéger contre des incidents ?

Les mesures de prévention et de protection décrites dans ce document n'ont pas l'ambition d'être exhaustives, ni d'être obligatoires dans tous les cas de figure. Le choix d'application des mesures de prévention et de protection doivent résulter d'une étude incluant une analyse de risques, confrontée à une évaluation budgétaire des parades adaptées.

Pour assurer l'efficacité de toutes les mesures de prévention et de protection proposées, il est indispensable de les inclure dans le cadre d'une approche organisationnelle et procédurale.

Les aspects suivants font l'objet de ce chapitre :

- ➔ Les dégâts des eaux.
- ➔ Les dégâts du feu.
- ➔ Les dégâts liés à l'électricité.
- ➔ Les défauts de climatisation.
- ➔ Les incidents de télécommunication.
- ➔ Les intrusions physiques.
- ➔ Les phénomènes électrostatiques.
- ➔ L'inaccessibilité du centre informatique.

4.1 Les dégâts des eaux

4.1.1. LES INCIDENTS

Ce type d'incidents peut avoir des origines diverses telles que :

- ➔ Rupture de conduite d'eau domestique.
- ➔ Rupture de conduite de réfrigération.
- ➔ Infiltration de façade ou de toiture.
- ➔ Déclenchement de systèmes anti-incendie.
- ➔ Obstruction des évacuations d'eaux usagées.

➔ REMARQUE :

Ce point est d'autant plus critique que la plupart des salles informatiques sont équipées de faux-planchers qui ne permettent pas une détection aisée d'un sinistre. De plus, les gainages de câblage entre les étages sont des évacuations faciles pour l'eau qui se peut se propager ainsi dans toutes les salles «connectique».

→ suite

4.1.2. LES CONSÉQUENCES

Les conséquences vont évidemment dépendre de l'ampleur du sinistre, mais on peut dire que les domaines susceptibles d'être touchés sont :

- Divers courts-circuits entraînant la rupture de service des équipements.
- Dangers d'électrocution.
- Dysfonctionnement de certaines alarmes ou autres sécurités.
- Détérioration des équipements.
- Corrosion des câbles et connecteurs.

4.1.3. LES CONTRE-MESURES

Prévention

- Choisissez judicieusement la localisation des locaux informatiques, en évitant les risques d'inondation (évités les sous-sols, évitez le dernier étage...).
- Limitez la circulation d'eau dans la salle informatique (placez le groupe de conditionnement d'air en dehors de la salle informatique...).
- Choisissez les chemins de tuyauterie, en évitant de traverser ou de surplomber la salle informatique.

Protection

- Mettez en place des systèmes de détection de fuites.
- Surélevez les équipements informatiques.
- Utilisez des tubes hermétiques pour le câblage d'alimentation (220V), ainsi que pour le câblage réseaux.
- Compartimentez le plancher de manière à contenir et diriger l'eau vers des systèmes d'évacuation.

4.2 Les dégâts du feu

4.2.1. LES INCIDENTS

Ce type d'incidents, qu'ils soient d'origine accidentelle ou criminelle, peut conduire à la destruction partielle de la société et plus particulièrement des équipements informatiques.

4.2.2. LES CONSÉQUENCES

Les conséquences de ce type de sinistre peuvent être très importantes à tous les niveaux de la société et non pas uniquement de l'informatique. En ce qui concerne le système informatique, cela peut causer l'indisponibilité de tout ou partie de l'architecture

et ce pour une assez longue période. Les dommages sont souvent couplés à des dégâts des eaux causés par les tentatives d'extinction de l'incendie et à des dégâts causés par les fumées.

Les dégâts habituellement constatés sont de différents types tels que :

- Destruction totale ou partielle du centre informatique.
- Destruction totale ou partielle du câblage cuivre et fibre optique.
- Dégâts liés à la pollution par la fumée et par les produits d'extinction.
- Atteintes physiques aux équipements informatiques.

4.2.3. LES CONTRE-MESURES

Prévention

- Prenez en compte le voisinage des bâtiments.
- Évitez le stockage de produits inflammables dans, ou à proximité des salles informatiques.
- Vérifiez régulièrement les circuits électriques.
- Évitez les chapelets de blocs « multiprises ».
- Mettez en place de mécanismes de détection de fumée.
- Étudiez les chemins de propagation du feu et mettez en place des équipements de compartimentage (sas, parois anti-feu...).

Protection

- Mettez en place de mécanismes d'extinction de feu sur base de produits ne portant pas préjudice au matériel informatique et ne portant pas atteinte au personnel (se renseigner auprès du service des pompiers de la localité).
- Choisissez judicieusement les sorties de secours.
- Faites respecter l'interdiction de fumer.
- Établissez et mettez à l'épreuve un plan catastrophe, incluant un repli de l'informatique vers un centre spécifique.
- Utilisez des armoires ignifugées pour le stockage des supports informatiques (veillez à garder ces armoires fermées).

4.3 Les dégâts liés à l'électricité

4.3.1. LES INCIDENTS

Les incidents électriques peuvent se manifester par des perturbations du courant sous forme de surtension, de baisse de tension, voire de coupures de courant. Ce type de coupure peut affecter tout ou partie de la société et peut être d'origine interne ou externe.

suite au verso →

→ suite

Malheureusement, l'apparition et la durée de ces phénomènes ne peuvent presque jamais être prévues, sauf dans les cas de coupure annoncée par le fournisseur ou par le service logistique en charge du bâtiment.

Une coupure de courant peut être malveillante ou résulter d'une fausse manœuvre, mais aussi être causée par des phénomènes naturels tels que les orages, les tempêtes...

4.3.2. LES CONSÉQUENCES

Le risque de dommages dépend de la brutalité de la coupure de courant, car certains équipements sont capables de gérer ce type de phénomènes de manière à clôturer sagement les transactions en cours.

Les conséquences peuvent être diverses :

- Perte de données.
- Panne d'équipements.
- Risques d'incendie.
- Electrocutation du personnel.

REMARQUE :

Il ne faut pas oublier que les équipements de connectique distribués dans les étages ainsi que les ordinateurs personnels et périphériques sont également des éléments critiques souvent très sensibles aux coupures de courant.

4.3.3. LES CONTRE-MESURES

Prévention

- Veillez à rendre les circuits d'alimentation au niveau du câblage électrique redondants.
- Veillez à une conception adéquate de l'alimentation électrique (tableaux, puissance...).
- Équipez les éléments critiques de l'informatique d'une double alimentation.
- Mettez en place des mesures visant à éviter les blocs « multiprises ».
- Équipez le bâtiment d'un mécanisme évitant les remontées de « foudre ».
- Installez des paratonnerres.

Protection

- Mettez en place des circuits de secours en cas de rupture (groupe électrogène).

- Mettez en place des circuits « no break » dans l'ensemble du bâtiment pour y connecter les machines et périphériques sensibles.
- Utilisez des solutions UPS (Uninterruptible Power Supply) avec logiciel d'alarme dans les salles ne pouvant fournir de circuit de secours.

REMARQUE :

On peut souvent remarquer que le problème de coupure de courant se prolonge lors du redémarrage. En effet, les équipements, tentant de redémarrer tous ensemble créent une surcharge qui fait sauter les fusibles. Il est conseillé de procéder à un redémarrage séquentiel des équipements.

4.4 Les défauts de climatisation

4.4.1. LES INCIDENTS

Les équipements informatiques sont conçus pour travailler dans un environnement spécifique qu'il faut respecter, afin d'éviter les incidents suivants :

- Défaut de fonctionnement de l'approvisionnement en eau ou en courant de réseau.
- Panne ou dysfonctionnement du système de réfrigération.
- Effets du rayonnement solaire direct.

4.4.2. LES CONSÉQUENCES

Il faut veiller à respecter les conditions normales de fonctionnement, sous peine de s'exposer à divers dysfonctionnements aléatoires difficiles à diagnostiquer. Toutefois, on peut dire que les conséquences habituelles d'une panne de climatisation sont les suivantes :

- Nécessité de couper et de redémarrer les équipements de façon cyclique.
- Vieillesse prématurée des composants informatiques.
- Détérioration des batteries de secours des UPS.

4.4.3. LES CONTRE-MESURES

Prévention

- Mettez en place des mécanismes veillant à limiter le rayonnement solaire direct.
- Installez un système de ventilation redondant, dimensionné correctement à pouvoir suffire aux besoins actuels et futurs.
- Mettez en place une solution de contrôle de la température équipée d'un module d'alerte.

[→ suite](#)

Protection

- Mettez en place des mécanismes permettant d'ouvrir la salle informatique en cas de nécessité.
- Mettez en place une procédure de passage en mode dégradé autorisant la coupure d'éléments informatiques non essentiels.

4.5 Les incidents de télécommunication

4.5.1. LES INCIDENTS

Parmi ce genre d'incidents, on peut citer les suivants :

- Sabotage.
- Panne ou perte d'équipement.
- Perturbation du signal.
- Rupture des canaux de liaison.
- Rupture de service d'un fournisseur.
- Panne d'un central téléphonique.

On inclut ordinairement sous ce nom d'autres incidents que ceux touchant directement les éléments physiques, comme les intrusions logiques sur les systèmes informatiques. Ceux-ci ne font pas l'objet de la présente fiche.

4.5.2. LES CONSÉQUENCES

L'impact dépend évidemment de l'usage qui est fait des services touchés dans les chaînes de production critiques.

Les conséquences sont les suivantes :

- Rupture de fonctionnement de certains logiciels.
- Isolation de la société par rapport au monde extérieur.
- Corruptions éventuelles de données.
- Désactivation de certains mécanismes de surveillance (vidéo, alarme...).

4.5.3. LES CONTRE-MESURES

Prévention

- Protégez judicieusement les locaux de télécommunication.
- Appliquez des gaines blindées aux liaisons extérieures (blindage, avertissement, bornes...).
- Séparez les gainages de courant fort, courant faible et les conduits de climatisation.
- Protégez les équipements de communication (antennes...) contre la foudre.

Protection

- Mettez en place des liaisons « doubles » avec chemins d'accès séparés, et au travers de deux centraux différents.
- Doublez tous les équipements critiques et mettez en place des systèmes de répartition des charges.
- Mettez en place des liaisons de secours quand c'est possible.
- Ayez recours à plusieurs opérateurs capables d'assurer le passage, en cas de rupture de service.

4.6 Les intrusions physiques

4.6.1. LES INCIDENTS ET CONSÉQUENCES

La circulation de personnes non autorisées dans les locaux informatiques (et dans les locaux de la société) peut mener à divers événements non désirés tels que :

- Vol de matériel.
- Perte de confidentialité.
- Sabotage.

4.6.2. LES CONSÉQUENCES

Les conséquences peuvent être les suivantes :

- Perte de réputation (mise en cause de la crédibilité dans le cas de divulgation d'informations hautement confidentielles...).
- Pertes financières directes (destruction de données cruciales, mise hors service de tout le système informatique...).
- Perte de temps (efforts pour rétablir les données détruites...).

4.6.3. LES CONTRE-MESURES

Dans ce domaine particulièrement, il est indispensable d'encadrer toutes les parades avec des mesures organisationnelles, procédurales et d'audit.

Prévention

- Mettez en place une protection générale du bâtiment (blindage, « bunker »...) avec limitation du nombre d'ouvertures (fenêtres, portes...).
- Utilisez un service de détection de déplacements et d'intrusions relié à une centrale de contrôle 24h/24h.
- Mettez en place un contrôle d'accès (badge, biométrie...) permettant de contrôler et de tracer les accès aux locaux critiques.
- Mettez en place une politique d'identification des visiteurs.

[suite au verso →](#)

→ suite

Protection

- Utilisez des mécanismes antivol pour les périphériques et les ordinateurs personnels ou portables.
- Veillez au respect d'une politique du bureau en ordre (clean desk), qui demeure une mesure limitant au maximum le risque de vol de données ou de matériels.
- Mettez en place un mécanisme de surveillance vidéo.

REMARQUE :

Avant d'implémentation ces mesures de surveillance veuillez en demander l'autorisation auprès de la Commission Nationale pour la Protection des Données.
(Art. 11 de la loi du 2 août 2002)

4.7 Les phénomènes électrostatiques

4.7.1. LES INCIDENTS

Tous les phénomènes électromagnétiques et électrostatiques sont regroupés sous cette appellation.

Ces perturbations peuvent provenir d'une source extérieure à la société, dans le cas de phénomènes météo, d'émissions radios ou d'appareillages électriques divers. La source peut également être liée au bâtiment.

4.7.2. LES CONSÉQUENCES

Les conséquences peuvent être les suivantes :

- Dysfonctionnements aléatoires.
- Corruptions de données stockées sur des supports magnétiques.

REMARQUE :

Un autre phénomène est l'utilisation des rayonnements émis par le système informatique pour intercepter des données. C'est le cas des réseaux « wireless », par exemple.

4.7.3. LES CONTRE-MESURES

Prévention

- Installez les locaux informatiques (traitement et connectique) éloignés des installations électriques, des ascenseurs et des autres sources de perturbation.

- Utilisation de fibre optique dans les liens verticaux (p.ex. entre les différents étages), de manière à limiter les risques.
- Mettez à la terre de tous les équipements et non pas uniquement des composantes informatiques.
- Choisissez judicieusement les revêtements des sols.

Protection

- portez des bracelets de mise à la terre pour toutes les interventions sur l'architecture informatique.

4.8 L'inaccessibilité du centre informatique

4.8.1. LES INCIDENTS

L'accès au centre informatique peut être rendu impossible pour plusieurs raisons telles que :

- Catastrophes naturelles et attentats.
- Décisions judiciaires suite à un sinistre.
- Manifestations, émeutes et mouvements sociaux.

4.8.2. LES CONSÉQUENCES

Les conséquences de l'incapacité d'accès peuvent être diverses :

- Arrêt de fonctionnement du centre de traitement.
- Altération du bon fonctionnement des équipements, spécifiquement des équipements sensibles.

4.8.3. LES CONTRE-MESURES

Prévention

- Installez vos sites là où les risques de catastrophes naturelles sont réduits.
- Mettez en oeuvre des protections contre les intrusions.

Protection

- Mettez en place une solution de prise de contrôle à distance sécurisée.
- Prévoyez la possibilité de passage sur un site de repli.

CASES,

pour plus de sécurité dans l'utilisation des systèmes d'information électroniques. Une initiative européenne soutenue par l'Etat luxembourgeois

OLAS

OFFICE LUXEMBOURGEOIS
D'ACCREDITATION ET DE
SURVEILLANCE



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Economie
et du Commerce extérieur