JORF n°303 du 30 décembre 2004

Texte n°7

ARRETE

Arrêté du 23 décembre 2004 relatif à la protection physique des informations ou supports protégés

NOR: PRMX0407871A

Le Premier ministre,

Sur la proposition du secrétaire général de la défense nationale,

Vu l'ordonnance n° 59-147 du 7 janvier 1959 modifiée portant organisation générale de la défense ;

Vu le décret n° 78-78 du 25 janvier 1978 fixant les attributions du secrétaire général de la défense nationale ;

Vu le décret n° 98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale, notamment l'article 6 ;

Vu l'arrêté du 25 août 2003 relatif à la protection du secret de la défense nationale et l'instruction générale interministérielle 1300/SGDN/PSE/SSD qui lui est annexée,

Arrête :

Article 1

La directive n° 1223/SGDN/SSD du 23 décembre 2004 sur la protection physique des informations ou supports protégés, ci-après annexée, est approuvée.

Article 2

La directive n° 1223/SGDN/SSD/DR du 17 décembre 1984, modifiée le 20 novembre 1990, sur la protection matérielle des documents classifiés est abrogée.

Article 3

Le présent arrêté sera publié au Journal officiel de la République française.

Article Annexe

A N N E X E

DIRECTIVE N° 1223 DU 23 DÉCEMBRE 2004 SUR LA PROTECTION

PHYSIQUE DES INFORMATIONS OU SUPPORTS PROTÉGÉS

Introduction

L'instruction générale interministérielle n° 1300 (IGI 1300) approuvée par arrêté du Premier ministre en date du 25 août 2003 fixe les règles générales de la protection du secret de la défense nationale. Elle définit, en particulier, les grandes lignes des mesures à mettre en oeuvre pour assurer la protection physique des informations ou supports protégés, quel que soit leur type, qui doivent être complétées par des mesures de sécurité spécifiques et détaillées.

La présente directive n° 1223 annule et remplace celle du 17 décembre 1984 modifiée. Elle s'inscrit dans un cadre de sécurité globale et complète l'IGI 1300. Elle décline les règles pratiques de protection physique à appliquer pour protéger les informations ou supports protégés contre toute menace d'origine interne et externe qui mettrait en cause leur disponibilité, leur intégrité, leur confidentialité et pour empêcher qu'une personne non autorisée y accède.

Par « protection physique », il est entendu l'ensemble des mesures de sécurité destinées à garantir l'intégrité des bâtiments, des locaux spécifiquement dédiés aux informations ou supports protégés et la fiabilité des meubles où ils sont conservés, afin d'éviter toute perte, dégradation ou compromission. Le degré de sécurité physique à mettre en oeuvre pour assurer leur protection doit être lié à leur niveau de classification, à leur volume et aux menaces auxquelles ils sont exposés.

Par « informations ou supports protégés », il est entendu les renseignements, procédés, objets, documents, données informatisées ou fichiers présentant un caractère de secret de la défense nationale (art. 1er du décret n° 98-608 du 17 juillet 1998).

Les éléments participant à la sécurité physique d'un système d'information figurent en annexe à la présente directive.

Le non-respect des modalités de la protection physique des informations ou supports protégés par leurs autorités détentrices engage leur responsabilité. Elles concernent tant les informations ou supports nationaux que les informations ou supports étrangers qui ont été confiés aux autorités françaises par les accords de sécurité bilatéraux et multilatéraux.

I. - Les principes généraux de la protection physique

La protection physique est assurée par un ensemble de mesures qui visent à empêcher toute intrusion dans les lieux où sont conservés les informations ou supports protégés et à tenter de s'assurer du ou des auteurs de cette intrusion.

Cet ensemble se compose de trois éléments combinés ou dissociés en fonction du niveau de classification :

- un ou plusieurs dispositifs de protection (les obstacles) ;

- un ou plusieurs dispositifs de détection et d'alarme ;

- des moyens d'intervention articulés autour de procédures et de consignes préétablies.

En retardant l'intrusion (aucun obstacle n'est infranchissable), un dispositif de protection satisfaisant a pour objectif de permettre la mise en oeuvre des moyens d'intervention, alertés et guidés par les dispositifs de détection.

Les mesures de protection physique comprennent :

- des mesures statiques à base de dispositifs matériels. Elles constituent l'essentiel des moyens de détection (tels que radar volumétrique, contact d'ouverture et sismique) et assurent la protection passive et active. Elles incluent aussi l'installation de systèmes de contrôle d'accès hiérarchisés selon le besoin d'en connaître (tels que badge, lecteur biométrique) ;

- des mesures dynamiques mettant en jeu des personnes (gardes, rondes de surveillance, filtrage, éléments d'intervention présents sur le site ou extérieurs) qui assurent l'intervention adéquate en contribuant à la détection par des actions de surveillance ;

- des mesures technologiques nouvelles dont l'emploi devra être parfaitement connu, testé par les utilisateurs et, le cas échéant, complété par des procédés mécaniques plus traditionnels ;

- des dispositifs technologiques nouveaux dont l'emploi devra être parfaitement connu, testé par les services spécialisés des ministères de la défense et de l'intérieur, éprouvé par les utilisateurs et, le cas échéant, complétés par des mécanismes plus traditionnels.

II. - La protection physique des informations

ou supports protégés : des barrières et des classes

Le système de protection de toute information ou support protégé est constitué de plusieurs « barrières » cohérentes, inclusives et successives : l'emprise du bâtiment, et/ou le bâtiment lui-même, le local qui contient le meuble, le meuble dans lequel est conservé l'information ou le support protégé.

Le niveau de protection d'ensemble est fonction du niveau de protection assuré par les dispositifs appliqués à chacune de ces « barrières ». Pour définir un seuil minimal de protection physique, il est donc nécessaire de classer chacune des barrières en fonction du degré de résistance qu'elle oppose aux tentatives d'intrusion.

La sécurisation physique des accès d'énergie, des locaux techniques et des autocommutateurs participe également à la protection physique des informations ou supports protégés. Les différents éléments à prendre en compte pour un système d'information sont recensés en annexe à la présente directive.

En fonction des dispositifs de protection dont elles bénéficient, chacune des barrières peut être répartie en plusieurs classes.

1. Classes du bâtiment et/ou l'emprise

Classe 4 : enceinte protégée (clôture d'une hauteur supérieure à 2,15 m ou, dans le cas où les murs du bâtiment constituent l'enceinte, protection de toutes les ouvertures situées à moins de 5,50 m au-dessus du niveau du sol) mais absence de gardes permanents ou de dispositifs de détection-alarme.

Classe 3 : protections de la classe 4 plus les gardes permanents effectuant des rondes de surveillance dans les locaux et l'emprise ou un dispositif de détection-alarme relié à un élément d'intervention extérieur (gendarmerie, commissariat de police, société de gardiennage).

Classe 2 : protection de la classe 3 plus des dispositifs de détection-alarme (éclairage, télésurveillance, détection périmétrique ou périphérique) et présence de gardes permanents.

Classe 1 : protection de la classe 2 plus les dispositifs de détection-alarme pour les locaux (détection périphérique ou volumétrique) ou les meubles (détection ponctuelle).

Les dispositifs électroniques de filtrage ne peuvent pas à eux seuls garantir l'intégrité des accès aux bâtiments et/ou emprises. Ils doivent être obligatoirement complétés par des systèmes mécaniques de fermeture qui doivent être activés en dehors des heures normales d'occupation des bâtiments.

2. Classes du local

Les parois ainsi que les plafonds et les sols des locaux doivent avoir une résistance suffisante.

Classe d : local avec porte à serrure mécanique ordinaire, équipée d'une sûreté à clé dont, si possible, l'ébauche est protégée, et fenêtres sans protection.

Classe c : local avec porte à serrure mécanique de haute sécurité (multipoints), équipée d'une sûreté à clé dont l'ébauche est protégée et fenêtres protégées lorsqu'elles sont situées à moins de 5,5 m d'un lieu accessible (sol, toit, corniche, descente d'eau pluviale).

La protection des fenêtres doit être assurée :

- soit par des barres en acier de 2 cm de diamètre au moins, espacées de 11 cm au plus ;

- soit par un vitrage anti-effraction. Les fenêtres doivent être alors munies d'un dispositif de limitation d'ouverture de manière à empêcher toute intrusion.

Classe b : local avec porte renforcée (en bois plein ou recouverte de feuilles d'acier), équipée d'un système antidégondage à serrure mécanique de haute sécurité avec détecteur ou compteur d'ouverture ; les autres ouvertures doivent être protégées comme pour la classe c.

Classe a : chambre forte dont la porte sera équipée au minimum des systèmes de sécurité des armoires fortes de classe B. Les parois des locaux doivent avoir une résistance au moins équivalente à 15 cm de béton.

3. Classes du meuble

Les meubles de sécurité destinés à la conservation des informations ou supports protégés se répartissent en trois classes et ne pourront pas être ouverts frauduleusement sans effraction. Ils seront donc conçus pour que toute tentative d'ouverture illégitime laisse des traces visibles. Ils seront dotés de serrure mécanique satisfaisant à la norme maximale de sécurité de leur pays d'origine.

Classe C : armoire dite forte, à un ou deux battants, à structure métallique, au moins égale à 20/10° de millimètre, munie d'une serrure mécanique, à combinaison silencieuse et à manoeuvre discrète qui permet de s'affranchir de la contrainte de la dernière clé. Les battants doivent posséder un système d'accrochage du côté du pivot. Les pênes, inaccessibles de l'extérieur, ne doivent pas pouvoir être délogés.

Classe B : armoire forte de structure identique à la classe C possédant en plus :

Un blindage des organes essentiels dont la présence peut être vérifiée visuellement par démontage du foncet de porte ;

Un délateur, à déclenchement mécanique et thermique, bloquant définitivement les mécanismes d'ouverture en cas d'ouverture illégitime ;

Un plombage du foncet (face intérieure de la porte) permettant de détecter aisément un démontage ;

Un système à clé interdisant l'accès aux « trous changeurs » de la combinaison ;

Un système d'asservissement du dormant, interdisant la fermeture de la porte principale lorsque l'autre battant n'est pas condamné, s'il ne s'agit pas d'une porte à battant unique ;

Un compteur d'ouverture non falsifiable et non réutilisable protégé par le foncet ;

Une serrure mécanique à combinaison silencieuse et à manoeuvre discrète est à recommander. Si la serrure est électronique, elle doit être haut de gamme (1), posséder une mémoire permettant son audit et comporter une serrure mécanique à clé variable en supplément, prisonnière tant que le pêne de la combinaison et les pênes du meuble ne sont pas sortis portes fermées ;

Un système de tringlerie constitué de barres métalliques en acier et de renvois assurant sur la porte principale une répartition géographique de plusieurs pênes horizontaux et verticaux. La poignée, si elle existe, doit posséder un point de rupture pour éviter un effort trop conséquent sur la tringlerie, sa position doit permettre la visualisation immédiate de l'oubli de la fermeture ;

Les portes seront dépourvues de toute plaque de propreté ou enjoliveurs.

Classe A : coffre-fort blindé sur toutes ses faces, d'un poids minimum à vide de 500 kilogrammes ou, à défaut, fixé au mur, au sol ou sur une plaque métallique d'une dimension supérieure aux issues du local ; ce meuble devra comporter tous les systèmes de sécurité de la classe B et, en plus :

Une ou plusieurs serrures pouvant s'adapter à un nouveau jeu de clés (serrures mécaniques dites à clé variable) ;

Au moins une serrure dont la clé reste prisonnière à l'ouverture tant que le pêne de la combinaison et les pênes du meuble ne sont pas sortis porte fermée.

D'une manière générale, la marque et le numéro de série du meuble sont estampés de façon apparente, à l'extérieur de celui-ci, sur des parties fixes et mobiles. Le numéro de série et l'année de fabrication de chaque serrure figurent sur celles-ci.
(1) Serrure qui offre des possibilités de paramétrage d'ouverture et de fermeture. Elle offre la possibilité de varier les codes suivants les horaires et les utilisateurs. De plus, elle dispose d'un système d'audit intégré.

III. - Classe minimale d'un meuble

Les tableaux ci-après définissent, pour chaque niveau de classification, la classe minimale du meuble à utiliser pour assurer la conservation de toute information ou support protégés, en fonction de la classe du local, du bâtiment et/ou de l'emprise.

Certains systèmes d'information traitant des informations ou supports protégés ne pouvant être rangés dans un meuble, une politique de sécurité du système d'information doit permettre de garantir la protection des informations traitées par ce dernier.

1. Sur le territoire national

Niveau très secret-défense

Vous pouvez consulter le tableau dans le JO

n° 303 du 30/12/2004 texte numéro 7

Niveau secret-défense

Vous pouvez consulter le tableau dans le JO

n° 303 du 30/12/2004 texte numéro 7

Niveau confidentiel-défense

Vous pouvez consulter le tableau dans le JO

n° 303 du 30/12/2004 texte numéro 7

2. Sur un territoire étranger

Compte tenu de leur environnement particulier, les organismes détenteurs d'informations ou supports protégés doivent appliquer des mesures de protection équivalentes au niveau de classification supérieur. Ainsi, les informations ou supports protégés classifiés confidentiel-défense doivent bénéficier des mesures de protection du tableau secret-défense.

Les classes de protection physique fixées ci-dessus, en fonction des niveaux de classification des supports à protéger sont des seuils minimaux à respecter impérativement.

Pour être efficace, un système de protection physique doit être :

Multiple, c'est-à-dire comporter plusieurs dispositifs de protection successifs, de nature différente, associés ou combinés à un ou plusieurs dispositifs de détection-alarme reposant eux-mêmes sur des principes différents ;

Homogène, c'est-à-dire garantir la même efficacité en tous points, l'intrusion s'opérant toujours dans la zone de moindre résistance, la valeur d'un système est celle de son point le plus faible ;

Dissuasif, c'est-à-dire se présenter sous un aspect pouvant contribuer à réduire le risque d'une tentative d'intrusion ;

Contrôlé, c'est-à-dire être testé fréquemment afin d'être maintenu en état opérationnel ;

Traçable, c'est-à-dire permettre de fournir tout moyen pouvant apporter un historique de fonctionnement des différents systèmes de sécurité.

IV. - Consultation des services spécialisés

En raison de la diversité des dispositifs de protection disponibles sur le marché et de l'évolution constante des techniques utilisées, les autorités concernées peuvent, en cas de besoin, consulter les services spécialisés des ministères de la défense et de l'intérieur sur l'efficacité des matériels et des systèmes de protection qu'ils désirent installer.

Il est rappelé que :

Les serrures des meubles et des locaux doivent posséder un système mécanique et que les paramètres de combinaison doivent être mis en oeuvre par des moyens de nature mécanique également ;

Le bon fonctionnement des dispositifs statiques de protection doit être régulièrement contrôlé et testé ;

Les mesures réglementaires de l'IGI 1300 concernant la protection des clés, ou des dispositifs équivalents, et des paramètres de combinaison doivent être appliquées de façon rigoureuse.

Glossaire

IGI 1300 : instruction générale interministérielle n° 1300/SGDN/PSE/SSD approuvée par arrêté du Premier ministre en date du 25 août 2003.

IGI 900 : instruction générale interministérielle n° 900/SGDN/SSD/DR - n° 900/DISSI/SCSSI/DR sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées du 20 juillet 1993.

IGI 500 bis : instruction interministérielle relative au chiffre dans la sécurité des systèmes d'information n° 500 bis/SGDN/TTS/SSI/DR du 18 octobre 1996.

IGI 485 : directive d'installation des sites et des systèmes d'information (protection contre les signaux parasites compromettants) n° 485/SGDN/DCSSI/DR du 1er septembre 2000.

Serrure : mécanisme fixé à une porte ou à un meuble que l'on manoeuvre à l'aide d'une clé.

Sûreté : mécanisme de la serrure qui est directement activé par la clé. On parle de sûreté intégrée lorsque le bloc de sûreté est intégré à la serrure, de sûreté rapportée lorsqu'il est positionné à l'extérieur de la serrure.

Sécurité : la sécurité d'une serrure est son aptitude à résister à une ouverture non autorisée. Elle englobe la résistance de la sûreté (notamment crochetage, extraction) et la résistance de la serrure (notamment résistance mécanique des pênes, résistance au forçage).

A N N E X E

ÉLÉMENTS PARTICIPANT À LA SÉCURITÉ PHYSIQUE

D'UN SYSTÈME D'INFORMATION

Le responsable de la sécurité d'un système d'information (centres informatiques, réseaux locaux ou stations isolées) en dehors de toutes considérations directes relevant de la sécurité des systèmes d'information (cf. IGI 1300, 900, 500 bis et 485) doit assurer physiquement la confidentialité, l'intégrité, la disponibilité et la continuité du système.

Bien en amont et dans le cadre de la mise en place d'un système d'information, il y aura lieu de tenir compte, dans la mesure du possible (le site étant souvent imposé), des éléments suivants :

Le choix du site au regard des risques et vulnérabilités engendrées :

Les inondations, les zones sismiques, le degré kéraunique (sensibilité à la foudre), la constitution et la nature des sols ;

Son implantation au regard de l'environnement (notamment sources chimiques, entreprises à risques, zones aéroportuaires, partage du site ou du bâtiment) ;

La nature du plan local d'urbanisme ainsi que de son évolution au regard des futures implantations ;

La conception du site et la nature du ou des bâtiments enfermant le système d'information.

Les contraintes logistiques :

La disponibilité des moyens logistiques ainsi que leurs éventuels secours (notamment énergie, télécommunications, climatisation) ;

La proximité et la rapidité des divers moyens d'intervention et de secours (notamment gardiennage, police, pompiers) ;

La nature des voies d'accès ;

Les divers problèmes de nuisances engendrés par le système (notamment bruit d'aérothermes).

Les contraintes organisationnelles :

La nature des flux de personnes et de matériels ;

La disposition des locaux et la nature de leurs cloisonnements ;

La lutte contre l'incendie (détections, extinctions) ;

La disposition des matériels informatiques vis-à-vis des ouvertures (notamment fenêtres) ;

Les types et nature des contrôles d'accès avec ou sans centralisation.

Le respect des contraintes réglementaires, juridiques et autres :

L'application des normes (notamment ISO 7498-2-99, ISO 13335, NFC 13-100, 15-100) ;

Règlements divers ;

Règles de l'art ;

Etat de l'art, ce que l'on sait faire à ce jour ;

Code du travail ;

Préconisations des constructeurs et installateurs ;

Eventuellement, les préconisations des assureurs.

Les objectifs de sécurité :

Définition des objectifs de sécurité à atteindre ;

Evaluation des risques potentiels ;

Gestion des risques résiduels ;

La mise en cohérence des divers éléments entre eux ;

Les plages horaires de fonctionnement du système ;

Les horaires de présence des divers personnels ;

La continuité du service et son mode ;

L’indisponibilité partielle ou totale ;

Le degré de sécurité souhaité en fonction de la nature des applications (notamment conditions d’accès au système, autorisations, confidentialités). A cet effet, il y aura lieu de définir la ou les zones de sécurité, c’est-à-dire de déterminer ce qui est contrôlable à tout instant par l’entité concernée avec la prise en compte des possibilités au regard des différents piégeages éventuels, électromagnétiques (notamment chemins de câbles, locaux de répartition), acoustiques (notamment vitrages, murs) et intrusions ;

Type et nature des protections sur les données en ligne ;

Coût potentiel d’un incident (physique, logique) ;

Type, nature et lieu des sauvegardes (programmes, données) ;

Formation.

Les conditions d’entretien et de maintenance :

Procédures et consignes existantes ou à écrire (notamment cahier formalisé, mise à jour, validations et tests réguliers) ;

Formalisation des comptes rendus ;

Marchés de maintenance (notamment type, nature, délais d’interventions) ;

Formation.

Fait à Paris, le 23 décembre 2004.

Jean-Pierre Raffarin