

Table des matières

■	Préface	9
■	Avant-propos	11
1	Introduction à la sécurité de l'information	15
	1.1 Que recouvre la sécurité de l'information?	17
	1.2 Qu'est-ce qu'un système d'information sécurisé?	19
	1.3 Quelles sont les menaces qui pèsent sur la sécurité de l'information?	21
	1.4 Quel cadre juridique pour la sécurité?	22
	1.5 Comment sécuriser l'information?	23
	1.6 Qu'est-ce que la gestion de la sécurité de l'information?	24
	1.7 Qu'est-ce qu'un projet de sécurité?	26
	1.8 Conclusion	28
2	Le Règlement général sur la protection des données (RGPD)	29
	2.1 Qu'est-ce qu'une donnée à caractère personnel?	29
	2.2 Qu'est-ce qu'un traitement?	30
	2.3 Les grands principes du RGPD	31
	2.4 Les changements organisationnels induits par le RGPD	32
	2.4.1 Le consentement	32
	2.4.2 Droit d'accès, de rectification et d'oubli	33
	2.4.3 Le transfert de données vers l'étranger	33
	2.4.4 La notification des problèmes	33
	2.4.5 La nomination d'un délégué à la protection des données	34
	2.4.6 Le registre des traitements	36
	2.4.7 L'analyse d'impact	38
	2.5 Les étapes clés pour se mettre en conformité avec le RGPD	40
	2.5.1 Désigner un responsable du projet	40
	2.5.2 Réaliser un inventaire des données et des traitements	40
	2.5.3 Mener les premières actions	40
	2.5.4 Gérer les risques	41
	2.5.5 Intégrer pleinement la protection des données dans l'entreprise	41
	2.5.6 Documenter la conformité	41
	2.6 Conclusion	42

3	Les ressources humaines et la sécurité	43
	3.1 Les enjeux	43
	3.2 Quelques exemples de problèmes spécifiques.....	44
	3.3 Les mesures à mettre en œuvre.....	45
	3.3.1 Désigner un référent.....	45
	3.3.2 Impliquer les utilisateurs	46
	3.4 Conclusion	49
4	Le contrôle d'accès aux données	51
	4.1 Les enjeux	51
	4.2 Quelques éléments techniques	52
	4.3 Quelques exemples de problèmes spécifiques.....	54
	4.4 Les mesures à mettre en œuvre.....	56
	4.4.1 Définir les données à protéger.....	56
	4.4.2 Définir les accès aux données	58
	4.4.3 Contrôler les accès.....	59
	4.4.4 Se protéger des attaques	60
	4.4.5 Auditer les accès	61
	4.5 Conclusion	62
5	La protection du poste de travail	65
	5.1 Les enjeux	65
	5.2 Quelques exemples de problèmes spécifiques.....	66
	5.3 Les mesures à mettre en œuvre.....	68
	5.4 Conclusion	71
6	La sécurité des réseaux	73
	6.1 Les enjeux	73
	6.2 Quelques éléments techniques	73
	6.2.1 La technologie des réseaux.....	74
	6.2.2 Les protections du réseau	74
	6.3 Quelques exemples de problèmes spécifiques.....	75
	6.4 Les mesures à mettre en œuvre.....	76
	6.5 Conclusion	78
7	La sécurité dans le cloud	81
	7.1 Les enjeux	81
	7.2 Quelques éléments techniques	82
	7.3 Quelques exemples de problèmes spécifiques.....	84

7.4	Les mesures à mettre en œuvre.....	85
7.5	Conclusion	87
8	La sécurité en situation de mobilité.....	89
8.1	Les enjeux	89
8.2	Quelques exemples de problèmes spécifiques.....	90
8.3	Les mesures à mettre en œuvre.....	91
8.4	Conclusion	93
9	La sécurité physique et environnementale	95
9.1	Les enjeux	95
9.2	Quelques exemples de problèmes spécifiques.....	96
9.3	Les mesures à mettre en œuvre.....	97
9.4	Conclusion	101
10	La gestion des incidents.....	103
10.1	Les enjeux	103
10.2	Les étapes de la gestion d'incidents.....	103
10.2.1	Se préparer aux incidents	104
10.2.2	Détecter un incident.....	105
10.2.3	Traiter l'incident	106
10.2.4	Reprendre les activités	107
10.2.5	Tirer les enseignements.....	107
10.3	Plan de réponse aux incidents.....	108
10.4	Les mesures à mettre en œuvre.....	110
10.5	Conclusion	111
11	La gestion d'un projet de sécurité.....	113
11.1	Les enjeux	113
11.2	Gestion de la sécurité	114
11.2.1	Nature de la gestion de la sécurité de l'information.....	115
11.2.2	Étapes clés de la gestion de la sécurité	117
11.2.3	Référentiels	118
11.3	Le détail des étapes clés.....	118
11.3.1	Stratégie de sécurité	118
11.3.2	Politique de sécurité.....	120
11.3.3	Évaluation des risques	123
11.3.4	Traitement des risques	132
11.3.5	Identification des mesures et procédures.....	133
11.3.6	Mise en œuvre du plan de sécurité	135

11.3.7	Sensibilisation et formation	135
11.3.8	Évaluation de la sécurité	136
11.3.9	Maintenance de la sécurité	138
11.4	Conclusion	140
12	Fiches pratiques	141
12.1	Comment mener une campagne de sensibilisation à la sécurité? ..	141
12.2	Comment établir un bilan de sa sécurité?	142
12.3	Réseaux sociaux et sécurité de l'information	147
12.4	Comment porter plainte?	148
12.5	Comment constituer le registre des traitements pour le RGPD?	149
12.6	E-mailing & RGPD	150
13	Conclusion générale	153
13.1	La sécurité dans la PME: tableau récapitulatif des mesures	153
13.2	Pour aller plus loin	157
	Glossaire	159
	Bibliographie	161
	Annexes	163
	Annexe 1: les menaces génériques selon EBIOS	163
	Annexe 2: les impacts génériques selon EBIOS	166
	Annexe 3: les acteurs et les rôles de la sécurité de l'information	168