L’homologation de sécurité au RGS

17 Octobre 2019 – La Rochelle

CHARENTE-MARITIME CYBER SÉCURITÉ
CMCS 2019

Votre intervenant

d.alexandre@soluris.fr
Damien ALEXANDRE
DaalSoluris

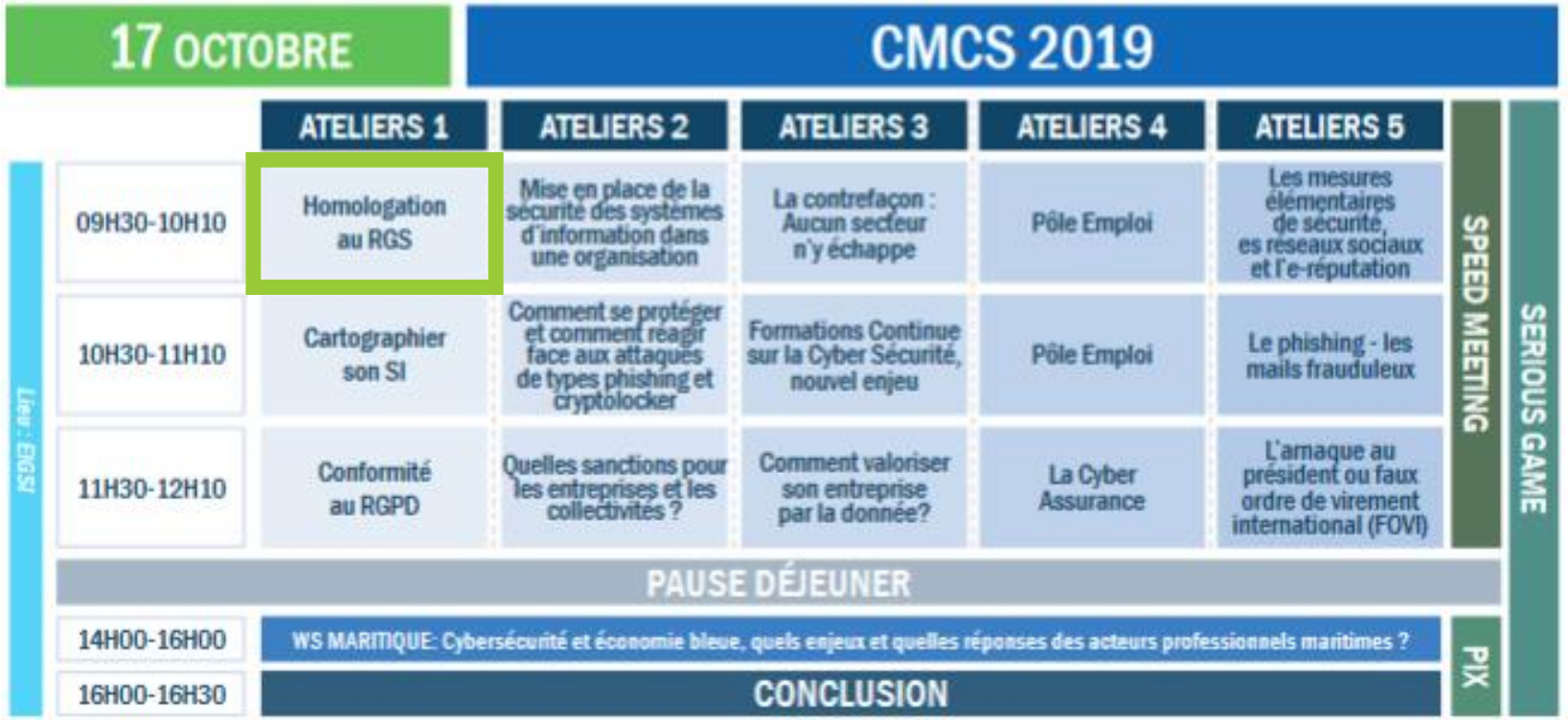
RSSI / DPO

Responsable du service confiance numérique

Membre du CLUSIF

Animateur de l’Espace CoTer

Vous êtes ICI



Qu’est-ce que le RGS ?

Le Référentiel Général de Sécurité

- Le référentiel général de sécurité (RGS) est le cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens.

CHAMP D'APPLICATION ET DESTINATAIRES

Le Référentiel général de sécurité **s'impose** spécifiquement aux systèmes d'information mis en œuvre par les **autorités administratives** dans leurs relations entre elles et dans leurs relations avec les usagers (il s'agit de téléservices tels le paiement de contraventions auprès de l'Administration).
Indirectement, le Référentiel général de sécurité s'adresse à l'ensemble des **prestataires de services** qui assistent les autorités administratives dans la sécurisation des échanges électroniques qu'elles mettent en œuvre, ainsi qu'aux industriels dont l'activité est de proposer des produits de sécurité.
De façon générale, pour tout autre organisme souhaitant organiser la gestion de la sécurisation de ses systèmes d'information et de ses échanges électroniques, le Référentiel général de sécurité se présente comme un guide de bonnes pratiques conformes à l'état de l'art.

CONTEXTE

Le référentiel général de sécurité est pris en application du **décret n° 2010-112 du 2 février 2010** pris pour l'application des articles 9, 10 et 12 de l'**ordonnance n° 2005-1516 du 8 décembre 2005** relative aux échanges électroniques entre les usagers et les autorités administratives.
Dans le cadre du développement des téléservices et des échanges électroniques entre l'administration et les usagers, les autorités administratives doivent garantir la sécurité de leurs systèmes d'information en charge de la mise en œuvre de ces services.
Le **RGS 2.0**, publié par un arrêté du 13 juin 2014, entre en vigueur au **1er juillet 2014**.
Le non-respect du RGS induit une faute de l'administration qui est susceptible d'engager sa responsabilité.

Liste des documents constitutifs du RGS v.2.0

CORPS DU RGS

- PDF Référentiel Général de Sécurité

DOCUMENTS APPLICABLES CONCERNANT L'UTILISATION DE CERTIFICATS ÉLECTRONIQUES

- PDF RGS A1 – Règles relatives à la mise en oeuvre des fonctions de sécurité basées sur lemploi de certificats électroniques, version 3.0
- PDF RGS A2 – Politique de Certification Type « certificats électroniques de personne », version 3.0
- PDF RGS A3 – Politique de Certification Type « services applicatifs », version 3.0
- PDF RGS A3 – Errata Horodatage électronique
- PDF RGS A4 – Profils de certificats, CRL, OCSP et algorithmes cryptographiques, version 3.0
- PDF RGS A5 – Politique d'Horodatage Type, version 3.0

https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/

Liste des documents constitutifs du RGS v.2.0

DOCUMENTS APPLICABLES CONCERNANT L'UTILISATION DE MÉCANISMES CRYPTOGRAPHIQUES

- RGS_B1_-_Règles_et_recommandations_concernant_le_choix_et_le_dimensionnement_des_mécanismes_cryptographiques,_version_2.03
- RGS_B2_-_Règles_et_recommandations_concernant_la_gestion_des_clés_utilisées_dans_des_mécanismes_cryptographiques,_version_2.0
- RGS B3 – Règles et recommandations concernant les mécanismes d'authentification, version 1.0 et version 2.0

RÉFÉRENTIEL D'EXIGENCES APPLICABLES AUX PRESTATAIRES D'AUDIT DE LA SSI

- RGS C – Référentiel d'exigences applicables aux prestataires d'audit de la SSI, version 2.0

https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/

Qui s’homologue au RGS ?

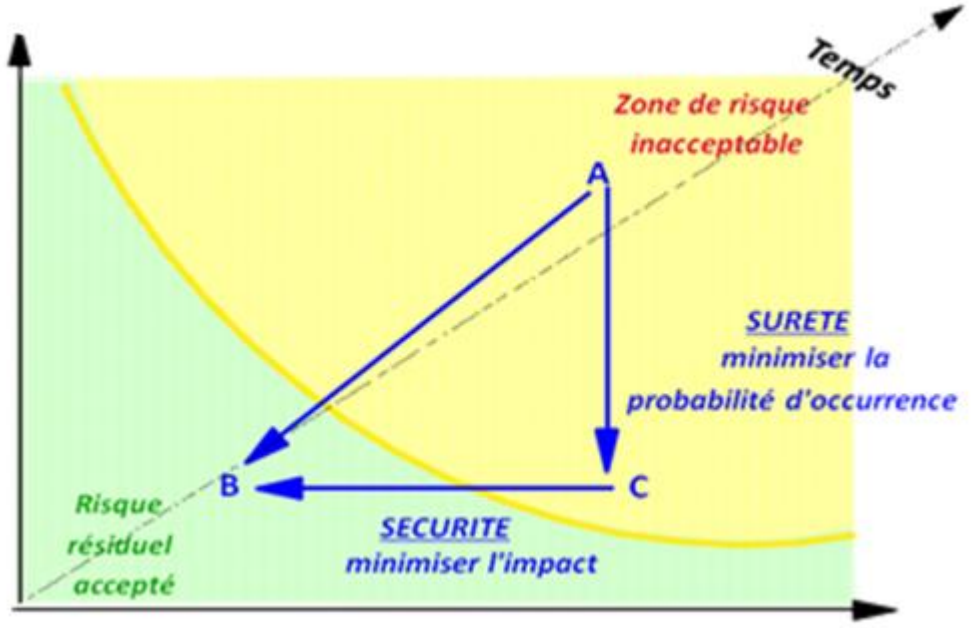
Les autorités administratives

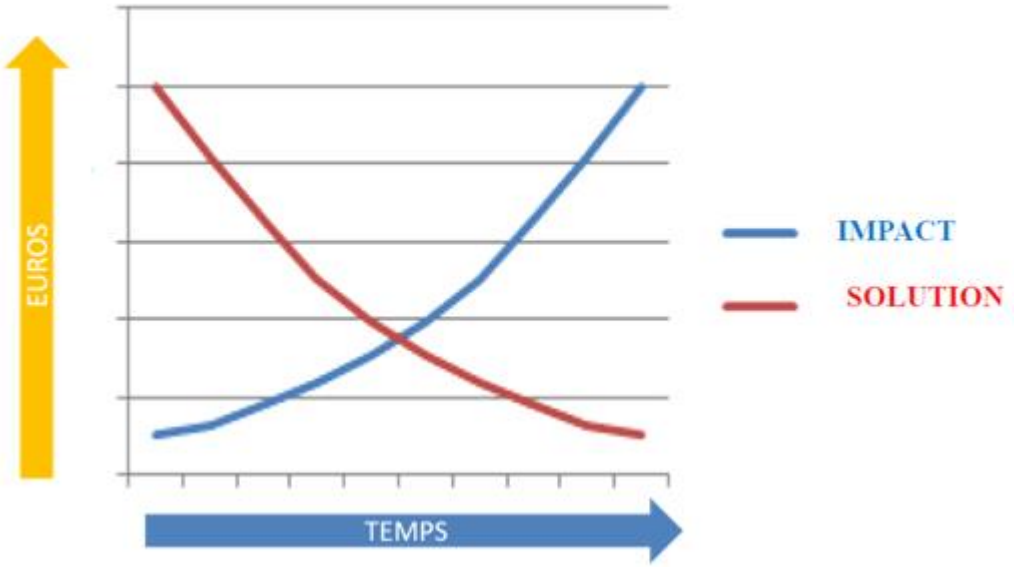
- Administrations d'état
- Collectivités territoriales
- Établissements publics à caractère administratif
- Organismes de gestion des régimes de protection sociale
- Organismes de gestion de services publics administratif

Pourquoi s’homologuer au RGS ?

Objectifs de l'homologation de sécurité

- de trouver un équilibre entre le risque acceptable et les coûts de sécurisation





Objectifs de l’homologation de sécurité

- de faire arbitrer cet équilibre, de manière formelle, par un responsable qui a autorité pour le faire.
- améliorer la sécurité pour un coût optimal, en évitant la « sur-sécurité », mais en prenant également en compte le coût d’un éventuel incident de sécurité.
- s’assurer que les risques pesant sur le SI, dans son contexte d’utilisation, sont connus et maîtrisés de manière active, préventive et continue.

Complémentarité avec le RGPD

CNIL.

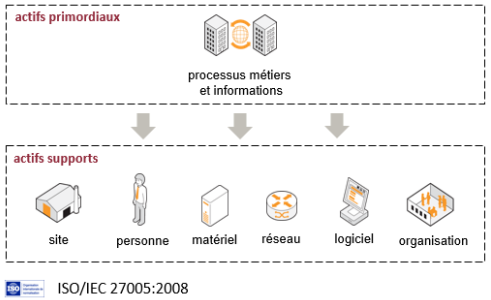
Référence : RGPD / LIL3
Référent : DPO
Inventaire des traitements
Analyse d'impact

Mesures de sécurité
techniques, organisationnels,
juridiques et humains

SMDCP

Gouvernance : Commission
Conformité RGPD

SYSTÈME D'INFORMATION



ISO/IEC 27005:2008

Vie privée des individus — Patrimoine de l'organisme

CONFIANCE NUMERIQUE

ANSSI

Référence : RGSv2
Référent : RSI ou RSSI
Inventaire des actifs
Analyse des risques

Mesures de sécurité
techniques, organisationnels,
juridiques et humains

SMSSI

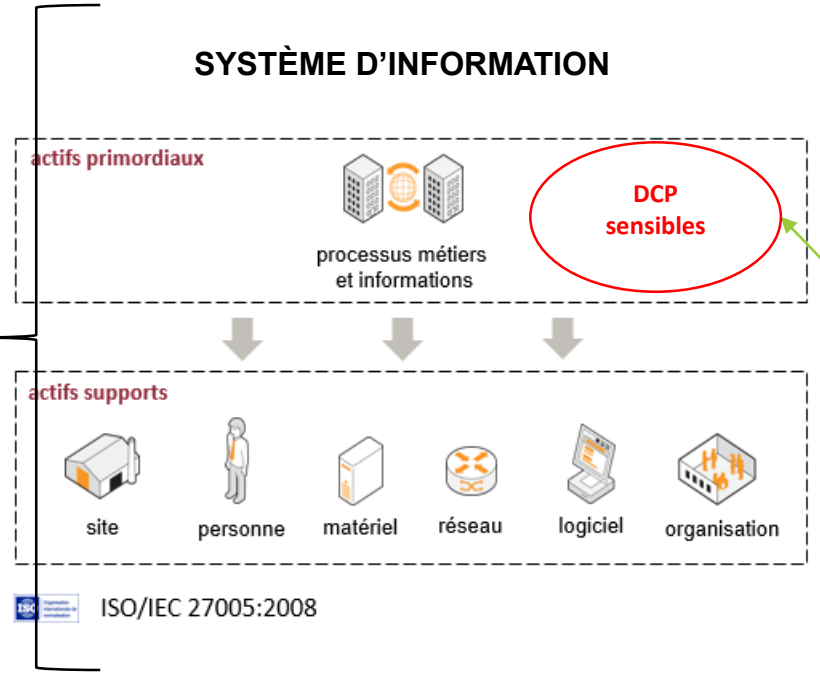
Gouvernance : Commission
homologation RGS

https://www.cnil.fr/fr/la-securite-des-donnees-des-administres

Complémentarité avec le RGPD

Risque		Maturité		
Type	Niveau	Niveau	Type	Mesures
Très fort	5	0 à 1	Informel	En réaction
Fort	4	1 à 2	Suivi	Planifiée
Marqué	3	2 à 3	Défini	Documentée
Limité	2	3 à 4	Contrôlé	Auditée
Faible	1	4 à 5	Optimisé	Amélioration continuelle

RGS



RGPD

Risque		Maturité		
Type	Niveau	Niveau	Type	Mesures
Très fort	5	0 à 1	Informel	En réaction
Fort	4	1 à 2	Suivi	Planifiée
Marqué	3	2 à 3	Défini	Documentée
Limité	2	3 à 4	Contrôlé	Auditée
Faible	1	4 à 5	Optimisé	Amélioration continuelle

Comment s’homologuer au RGS ?

L’homologation de sécurité en neuf étapes simples

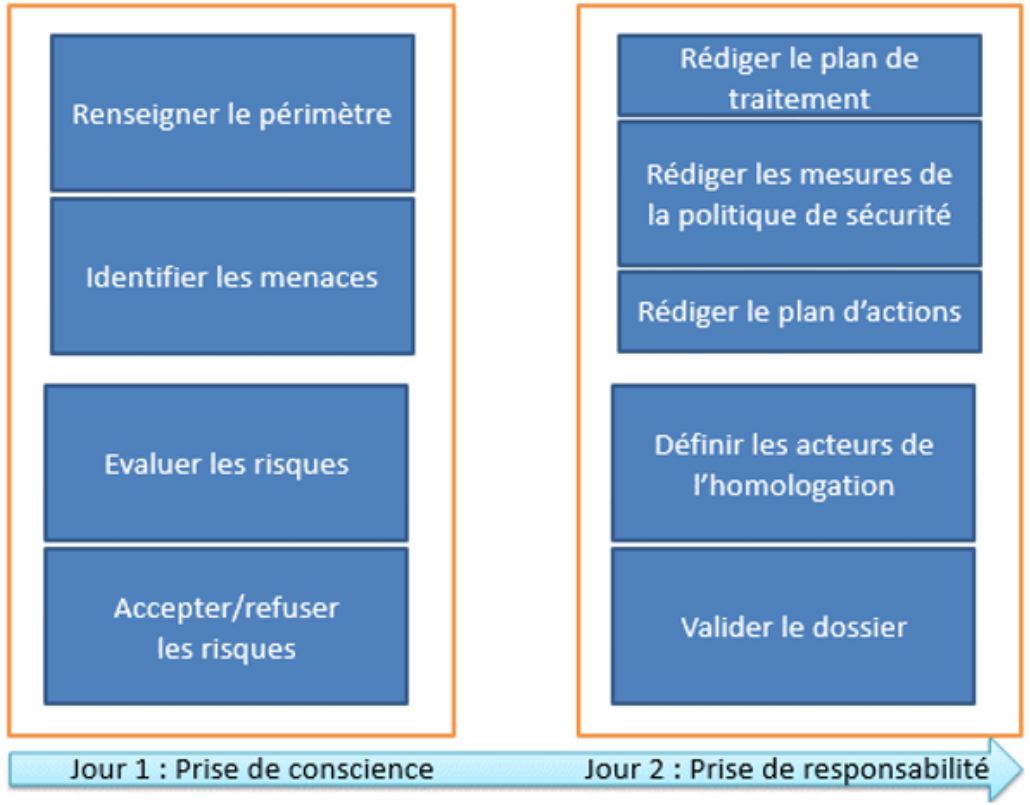
https://www.ssi.gouv.fr/administration/guide/lhomologation-de-securite-en-neuf-etapes-simples/

Le guide d'homologation de sécurité

Étape n° 1 : Quel système d'information dois-je faire homologuer et pourquoi ?
Étape n° 2 : Quel type de démarche dois-je mettre en œuvre ?
Étape n° 3 : Qui contribue à la démarche ?
Étape n° 4 : Comment s'organise-t-on pour recueillir et présenter les informations ?
Étape n° 5 : Quels sont les risques pesant sur le système ?
Étape n° 6 : La réalité correspond-elle à l'analyse ?
Étape n° 7 : Quelles sont les mesures de sécurité supplémentaires pour couvrir ces risques ?
Étape n° 8 : Comment réaliser la décision d'homologation ?
Étape n° 9 : Qu'est-il prévu pour continuer d'améliorer la sécurité ?

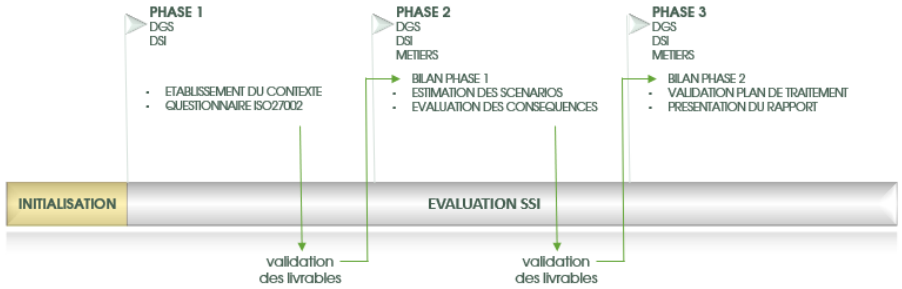
https://www.ssi.gouv.fr/uploads/2014/06/guide_homologation_de_securite_en_9_etapes.pdf

Déclinaison SOLURIS en 2 jours

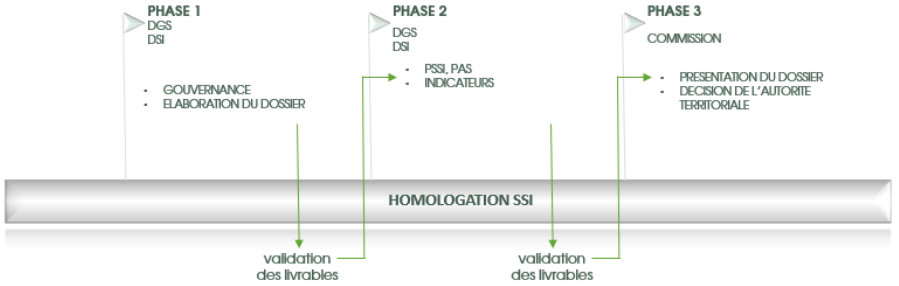


Déclinaison SOLURIS en 6 jours

Etape 1 : Analyse du risque

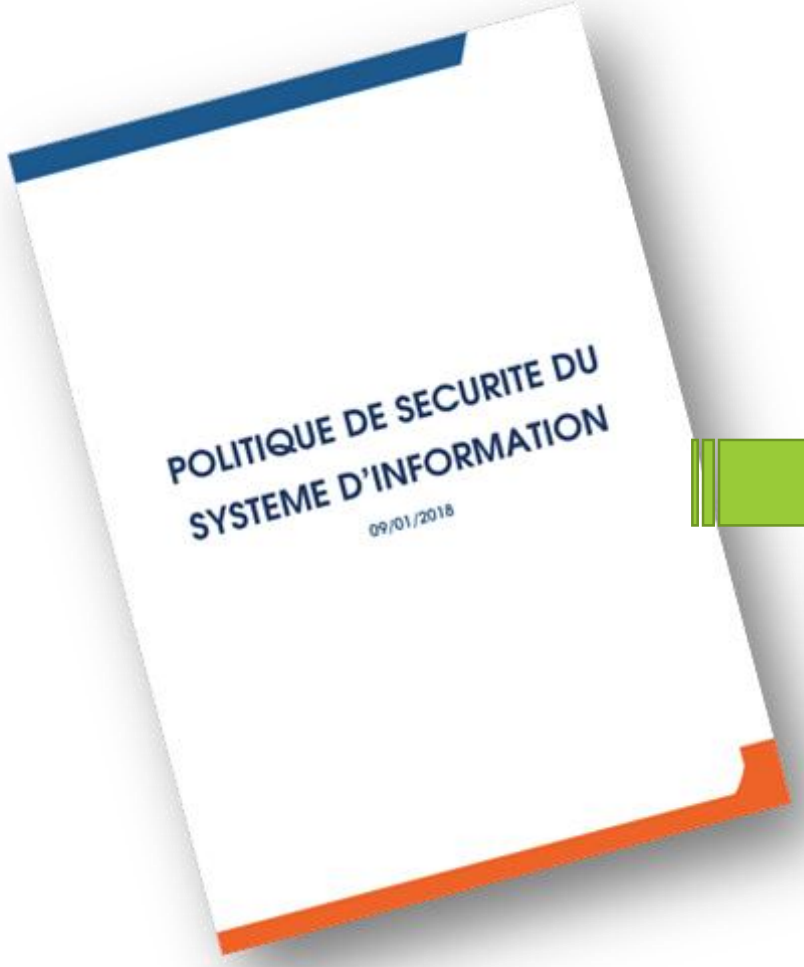


Etape 2 : Cycle de vie



Les livrables communs aux 2 déclinaisons

La Politique de Sécurité du Système d'Information



https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/

Merci
et
bon colloque