SCHEMA DIRECTEUR DE SECURITE

1. Introduction :

Un schéma directeur (plan directeur) est un document dynamique de planification à long terme (mis à jour périodiquement) qui fournit une disposition conceptuelle pour guider la croissance et le développement futurs. Il est développé dans le but de faire orienter la politique de l'entreprise dans le futur, en précisant les axes prioritaires à développer (les projets futurs), sur lesquels l'entreprise doit s'appuyer afin de s'adapter aux changements technologiques.

Si l'objectif d'un Schéma Directeur a toujours été d'offrir une vision à long terme pour tendre vers un objectif en phrasant les évolutions et les dépenses budgétaires, aujourd'hui la notion de « long terme » est remise en question avec l'évolution des modes de consommation, l'accélération des avancées technologiques et l'arrivée de nouveaux acteurs plus rapides et plus agiles qui remettent en question les hiérarchies établies depuis longtemps sur le marché.

Alors qu'il était commun d'établir un Schéma Directeur pour une période de trois à cinq ans et de mettre plusieurs mois à le réaliser, un Schéma Directeur moderne se doit d'être réalisé le plus rapidement possible et pour une période courte, en intégrant la même philosophie Agile que celle appliquée dans la Gestion de Projet.

Il en existe plusieurs types à savoir :

- Le schéma directeur stratégique (à dominante politique)
- Le schéma directeur informatique.
- Le schéma directeur du système d'information
- Le schéma directeur de la sécurité du système d'information
- Le Schéma Directeur numérique.
- …etc.

Le Schéma Directeur de Sécurité des Systèmes d'Information (SDS ou SDSSI) est une démarche méthodologique consistant à ouvrir périodiquement un grand chantier dans le domaine de la sécurité des systèmes d'information (SSI) dans l'optique :

- De vérifier que l'organisation mise en œuvre est opérationnelle et performante ;
- D'actualiser les axes d'orientation au regard des évolutions technologiques ;
- De mesurer l'adéquation entre les enjeux de la SSI et les risques encourus ;
- D'évaluer la compatibilité des moyens accordés avec les objectifs visés ;
- D'actualiser le plan d'action SSI.

Le Schéma Directeur de la Sécurité des Systèmes d'Information vise à :

- Expliciter les contextes de mise en œuvre du schéma directeur;
- Identifier et préciser les enjeux de la sécurité ;
- Offrir un cadre commun pour la définition et la mise d'œuvre des politiques de sécurité dédiées;
- Fixer les orientations techniques sous-jacentes aux projets de modernisation des systèmes d'information (SI) ainsi qu'au développement sécurisé de l'administration électronique;
- Traduire les objectifs de sécurité sous forme de plans d'actions opérationnels.

2. Cadre d'élaboration du SDSSI :

L'élaboration du schéma directeur de la sécurité doit prendre en considération différents contextes ; selon ces contextes les objectifs visés, les projets à définir et les stratégies suivies se multiplient et divergent.

2.1. Contexte politique et stratégique :

L'évolution rapide de la technologie de l'information et de la communication (tic) et la généralisation de son utilisation imposent aux entreprises d'ouvrir leurs systèmes d'information en accès à distance aux différents utilisateurs via différents types de matériel ; ce qui complique sans cesse la tache de sécurisation.

Ainsi le développement d'une politique de sécurité revêt un caractère stratégique pour chaque entreprise.

Par ailleurs les recommandations exigées par la loi envers la protection de l'information définit les grandes orientations de la politique de sécurité à mettre en œuvre en matière de sécurité des systèmes d'information, pour assurer la protection des informations sensibles non classifiées de défense, dans le respect des lois et règlements en vigueur.

2.2. Contexte juridique :

Le schéma directeur de la sécurité des systèmes d'information découle également d'une prise en compte au plus haut niveau de l'institution de l'évolution des réglementations publiques nationales et/ou mondiales. L'importance des TIC a été progressivement pise en compte par les lois dans presque le monde entier dès la fin des années 70. Ces règlements engagent la responsabilité de personnes physiques et morales envers la sécurité, et les obligent à prendre au sérieux la sécurité de leur SI en allant de la simple protection de la vie privée et jusqu'à encadrer l'économie numérique.

2.3. Contexte institutionnel et organisationnel :

Le schéma directeur de la sécurité des systèmes d'information doit prendre en considération aussi les spécificités des communautés territoriales, le partage des responsabilités défini dans le cadre de la loi.

Cette diversité doit être tenue comme étant une richesse et un avantage pour le développement du SDSSI, en encourageant la participation et l'implication des acteurs locaux à l'élaboration et la mise en œuvre des plans de sécurité, ainsi que l'adaptation des dispositions aux spécificités locales, départementales et régionales,

Cependant cette diversité ne doit être en aucun cas un frein à la formation et la sensibilisation de l'ensemble des usagers des ressources numériques.

2.4. Contexte technique :

L'évolution des moyens techniques est à l'origine d'une interaction forte entre systèmes d'information, systèmes informatiques et organisations.

Aujourd'hui, l'importance accrue des réseaux du fait d'un déploiement massif des postes de travail informatiques rend leur fiabilité et leur disponibilité impérative.

L'accroissement des performances des matériels, combinée aux fortes baisses de coûts, a progressivement amené les systèmes d'information à se substituer aux modes de travail traditionnels vers lesquels il ne saurait être envisageable de revenir, ne serait-ce que ponctuellement.

Cette nouvelle organisation tend à abolir la notion d'espace de travail géographiquement localisé, mais cette souplesse absolue nécessite d'imposer des mesures strictes de cloisonnement des réseaux comme de règles de confinement des zones d'interopérabilité.

La sécurité des systèmes d'information doit s'inscrire dans un cadre technique maîtrisé.

En plus la pandémie du COVID19 qu'a connu le monde entier dans cette période a imposé aux responsables des entreprises de formaliser de nouvelles modalités d'organisation du travail, à prendre les mesures adéquates pour assurer la continuité de l'activité en encourageant surtout le passage au télétravail, ce qui rend indispensable aux mesures de sécurité déjà mise en place de s'adapter à cette nouvelle situation, et de trouver de nouveaux mécanismes pour améliorer et renforcer la sécurité d'authentification et des accès à distance.

3. Les principales méthodes d'élaboration du Schéma Directeur

Il existe plusieurs méthodes de schémas directeurs, on peut citer :

3.1. La méthode BSP (*Business System Planning d'IBM*) :

C'est une méthode orientée opportunité d'investissement, développée au début des années 70 par IBM initialement à usage interne uniquement ; puis en 1981 IBM décida de la mettre à la disposition des clients. Plus tard, cette méthode est devenue un outil important pour de nombreuses organisations.

C'est une méthode très complexe qui se base sur l'analyse, la définition et la conception de l'architecture de l'information de l'organisation, en traitant les données, les processus, les stratégies, les objectifs et les départements organisationnels qui sont interconnectés.

Son objectif est de :

a. Comprendre les problèmes et les opportunités avec les applications et l'architecture technique actuelles.
b. Développer un état futur et un chemin de migration pour la technologie qui prend en charge l'entreprise.
c. Fournir aux dirigeants d'entreprise une direction et cadre de prise de décision pour les dépenses d'investissement informatiques.
d. Fournir au système d'information un plan de développement.

Le résultat d'un projet BSP est une feuille de route exploitable qui aligne les investissements technologiques sur la stratégie commerciale.

Les étapes du processus BSP sont :

1. Obtenir l'autorisation de l'étude
2. Constituer l'équipe d'étude
3. Définir les classes de données
4. Définir les processus métier
5. Définir l'architecture de l'information à l'aide de ces classes de données et processus métier.
6. Comparer cette architecture avec les systèmes actuels et identifier les systèmes manquants et/ou nécessaires.

7. Interroger la haute direction pour s'assurer que l'architecture est correcte et pour identifier tout problème.
8. Établir des priorités pour chacun des principaux systèmes contenus dans l'architecture
9. Préparer le rapport final de l'étude et le présenter au top management.
10. Si approuvé, lancer la construction de l'architecture

3.2. La méthode RACINES (*RAtionalisation des Choix INformatiquES*) :

C'est une approche structurée et rationnelle, surtout présente dans les administrations françaises dans les années 1970-1980 ;

Elle part du principe de laisser les structures mises en place mener elles-mêmes le processus d'élaboration du Schéma Directeur. Toutefois, tant que ces structures ne maîtrisent pas le savoir-faire, elles ont besoin d'être appuyées par un spécialiste de cette méthode. Cet expert, qui est généralement un Consultant, intervient pour communiquer son savoir-faire, principalement au groupe de projet, aux moments clés de l'opération Schéma Directeur, à travers de légères interventions de formation et de conseil. Il assure le suivi indirect de l'opération à travers la préparation des points de contrôles auxquels il ne participe pas toujours directement. L'opération doit être menée de telle sorte qu'une équipe interne soit capable de faire évoluer et d'améliorer le document Schéma Directeur, après avoir assimilé les principes de base.

Le processus RACINES complet, découpé en 5 étapes, permet d'étaler dans le temps les difficultés et de résoudre successivement les problèmes qui se posent.

- Étape I. Lancement de l'opération : définir précisément les rôles et les objectifs de l'opération, mettre en place les structures de travail et faire adopter un cahier des charges de l'opération.
- Étape II. Bilan de l'existant et orientations générales : analyser la situation et les besoins des utilisateurs, définir le système cible.
- Étape III. Scénarios : prévoir de manière volontaire mais réaliste en comparant plusieurs scénarios permettant d'atteindre le système cible.
- Étape IV. Plans d'actions annuels : décider en préservant l'adhésion, après avoir choisi l'un des scénarios, évaluer les différents projets.
- Étape V. Mise en œuvre et suivi de l'exécution du Schéma Directeur : faire exécuter de façon rigoureuse.

3.3. La méthode Nolan Norton :

La méthode Nolan Norton est une méthode opportuniste orientée Retour sur Investissement (ROI return On Investment), qui introduit notamment la notion de portefeuille applicatif ou Application Portfolio Management (APM). Elle peut se décomposer en sept étapes :

1. Comprendre les objectifs et les stratégies des métiers dans le but d'identifier les investissements informatiques générant les plus grandes opportunités de rentabilité.
2. Identifier les initiatives clés qui doivent être réalisées pour supporter les objectifs business.
3. La Direction détermine les éléments critiques de succès pour les investissements stratégiques en évaluant l'impact des fonctions clés sur chacune des initiatives stratégiques.
4. Identifier les programmes qui impactent le plus les objectifs métiers et les activités clés de l'organisation.

5. Les directions opérationnelles et les responsables informatiques doivent préparer conjointement les descriptions précises de chaque programme.
6. Le management doit revoir les ordres de priorité des programmes en fonction du niveau d'investissement fixé.
7. Développer les budgets et fixer des objectifs de performance basés sur la réussite du programme et les bénéfices obtenus

3.4. La méthode S-ISP *(Strategic - Information System Planning)* :

C'est une nouvelle ingénierie des systèmes information.

ISP est le processus d'exploration des tâches essentielles pour le développement des systèmes en étudiant les objectifs et le Business Plan de l'organisme.

- Planifier le projet de plan stratégique du SI
- Analyser les stratégies et les politiques existantes
  - Étudier la stratégie de l'organisme
  - Analyser l'organisation de l'information et des données
  - Analyser l'environnement technique actuel
  - Définir une architecture informationnelle préliminaire
- Identifier les exigences des métiers
  - Analyser les systèmes actuels et futurs
  - Déterminer les besoins et priorités en informations des métiers
- Définir l'architecture du SI
  - Définir l'architecture informationnelle
  - Définir l'architecture applicative
  - Définir la future organisation de la DSI
  - Définir l'architecture technique
- Finaliser la stratégie des SI
  - Définir les stratégies et les plans d'action
  - Obtenir l'adhésion des différents acteurs concernant le plan stratégique

4. Les projets et missions à définir :

2.1. La charte pour le personnel :

L'objectif est d'encadrer les conditions d'utilisation des ressources informatiques et systèmes d'information de l'entreprise par son personnel.

Exerçant une activité professionnelle au sein d'une entité relevant de la responsabilité d'une PJR, les personnels et autres intervenants (professionnels, associatifs...) se doivent de respecter la réglementation en général et tout particulièrement les règles de déontologie et de sécurité consignées dans la charte d'utilisation des ressources informatiques dont les PJR doivent assurer la diffusion.

En tant qu'utilisateur et/ou personnel de l'état, chaque individu est responsable en tout lieu et tout temps de l'usage qu'il fait des ressources informatiques, des réseaux ou des systèmes qui sont mis à sa disposition.

2.2. La charte de bon usage des moyens informatiques :

Charte établie par le RSSI et sert à cadrer l'usage des ressources. Elle contient par exemple des mesures concernant l'utilisation de l'internet, règles légales, de propriétés intellectuelles. La consultation de cette charte peut être désignée comme obligatoire (à signer individuellement) ou bien communiquée par la SDSSI sous différentes formes de sensibilisation envers la sécurité.

2.3. Gestion des traces informatiques :

Tracer l'activité des systèmes d'information est primordial pour une organisation. L'exploitation des traces peut être très efficace pour détecter les attaques, les activités inhabituelles ou inappropriées qu'elles soient d'origine interne ou externe, de déterminer l'étendue d'une intrusion éventuelle afin de la circonscrire, d'aider à la conduite d'enquête concernant les attaques détectées afin de pouvoir les neutraliser définitivement.

A cet effet, des moyens de traces informatiques doivent être mis en place, et une Charte de la gestion des traces informatiques doit être diffusée à l'ensemble de la communauté.

2.4. L'autorisation et les droits d'accès :

L'autorisation (gestion des droits) consiste à accorder à une identité numérique des droits d'accès correspondant à son profil ou à ses missions (rôles). Il est conseilléé ainsi d'organiser le personnel dans des groupes (espaces numériques de travail) et désigner à chacun selon ses prérogatives (poste et rôle joué) des mécanismes efficaces pour l'authentification et de lui attribuer les autorisations correspondantes.

Il est recommandé d'utiliser un annuaire de référencement unique afin d'établir l'identification de l'individu et de centraliser l'information..

2.5. La sauvegarde de l'information :

Les données sensibles doivent être sauvegardées (sur disques durs, bandes magnétiques, ..) afin de palier à un éventuel soucis, volontaire ou non. Ces copies de sauvegarde servent à pouvoir restaurer les données contenues dans les bases de données, les courriels, les pages web, etc.

2.6. Élaboration d'une PSSI :

Afin d'étendre son activité et offrir des services dans un cadre général et légal, il est important de mettre en place une Politique de Sécurité du Système d'Information, en y spécifiant des références réglementaires et légales claires et des consignes et procédures cohérentes.

Les procédures de contrôle et d'audit doivent être clairement définies sur la base de la transparence, de la discussion collective obligatoire avec les organes représentatifs du personnel et de la proportionnalité de mesures pouvant être prise en cas d'infraction en respect de la loi.

2.7. Elaboration d'un Plan d'Action Sécurité :

C'est la déclinaison opérationnelle du schéma directeur de la sécurité du Système d'Information.

Le plan d'action sécurité décrit ou met à jour pour l'année les tâches liées à la mise en œuvre de la sécurité des informations au sein de l'entreprise et il est ordonnancé en fonction des priorités, c'est à dire en fonction des besoins de sécurité calculés lors de l'analyse des risques.

Ceci implique donc de mettre en place au préalable une analyse des risques et des menaces puis de mettre en place une gestion des risques (obtenir une absence de risques inacceptables par la mise en œuvre de mesures de sécurité).

2.8. Elaboration d'un carnet de sécurité du système d'information :

Toute application ou système d'information doit disposer d'un carnet de sécurité. Ce carnet constitue l'outil de référence en matière de SSI.

Ce carnet a vocation à être renseigné tout au long du cycle de vie du SI par l'ensemble des acteurs impliqués dans le processus de développement et de l'exploitation des SI.

Chaque dossier de sécurité produit au cours du cycle de vie du SI se doit d'être intégré dans le carnet de sécurité, lequel sera partagé par tous les acteurs impliqués.

2.9. Désigner la chaîne de la sécurité opérationnelle des SI :

Il est souvent rappelé que les défaillances de sécurité trouvent leur cause, dans leur grande majorité, dans des comportements humains inappropriés. En conséquence, les utilisateurs internes des SI doivent être informés de leur responsabilité individuelle en matière de sécurité des systèmes d'information dans le cadre de leurs fonctions ou des missions qu'ils exercent au sein de l'établissement.

Ceci implique également que chacun puisse disposer des éléments d'informations organisationnels nécessaires pour faire face à des situations d'attaques logiques ou des perturbations du fonctionnement de leur environnement de travail.

Il s'agit donc bien, dans un premier temps, de recenser les acteurs concernés ou impliqués à quelque titre par cette problématique globale de sécurité.

Par convention, l'autorité hiérarchique est appelée «PJR».

a. PJR (*Personne Juridiquement Responsable*) :

La PJR *est de fait l'Autorité Qualifiée en Sécurité du Système d'Information (AQSSI)*. Pour exercer cette responsabilité, l'autorité hiérarchique doit s'appuyer sur le Responsable de la Sécurité des Systèmes d'Information (RSSI).

b. Le RSSI :

Le Responsable de la Sécurité des Systèmes d'Information est nommé par la «Personne Juridiquement Responsable».

A ce titre, le Responsable de la Sécurité des Systèmes d'Information conseille la «Personne Juridiquement Responsable» en matière de sécurité des systèmes d'information.

Les missions principales du RSSI sont les suivantes :

- Constituer et coordonner un réseau interne de correspondants de sécurité ;
- Mettre en place les plans de sécurité adaptés aux établissements et aux services ;
- Organiser le référencement des sites dangereux ou illicites au niveau de l'entreprise et assurer la mise à jour des dispositifs de filtrage en conséquence ;
- Contrôler régulièrement le niveau de sécurité du système d'information par l'évaluation des risques résiduels ;
- Informer et sensibiliser les utilisateurs du système d'information aux problématiques de sécurité ;

- Améliorer la SSI par une veille technologique active ainsi que par une participation aux groupes de réflexion ad hoc ;
- Assurer la coordination avec les différents organismes concernés.

Pour assurer pleinement toutes les composantes de sa mission, le RSSI s'appuie sur une chaîne de Correspondants de Sécurité qu'il organise et dont il est le référent.

c. Les usagers privilégiés du système d'information :

Situés dans la DSI, il s'agit des informaticiens ayant à la fois les connaissances et les privilèges d'accès aux ressources manipulés par les usagers du système d'information, que ce soit au niveau serveur, ou poste local.

Ils travaillent en collaboration avec les correspondants de sécurité, devant sensibiliser les usagers du SI et s'assurer de la bonne application et respect de la Charte de bon usage des moyens informatique. Ils sont tenus de remonter toute anomalie visant à porter atteinte à l'intégrité du SI aux correspondants de sécurité.

Les usagers privilégiés du SI sont soumis à une charte administrateurs informatique.

d. Les correspondants de sécurité :

Sous l'autorité de la PJR et l'appui nécessaire du RSSI, les Correspondants de Sécurité sont chargés de la mise en œuvre de la sécurité au sein d'une entité donnée. Ils ont une qualification informatique de niveau administrateurs systèmes et réseaux ou, à défaut, des compétences reconnues en la matière. Leur nombre peut varier selon la nature et la taille de l'entité dans laquelle ils évoluent.

Les Correspondants de Sécurité mettent en œuvre les règles générales d'exploitation, consignées dans le carnet de sécurité des systèmes d'information, pouvant être complétées par des mesures liées aux spécificités de l'entité.

Chaque correspondant de sécurité devra être désigné. Sa prise de fonction est accompagnée de la prise de connaissance d'une charte nationale «administrateurs» par laquelle il est informé de ses droits et devoirs. Dès lors, il s'engage à respecter cette charte qui est annexée au règlement intérieur de l'entreprise.

Tout correspondant de sécurité doit être identifié et associé à la politique de sécurité.

e. Les usagers du système d'information :

En bout de chaîne de SSI, on trouve les usagers du SI qui seront définis comme des entités ayant accès à des ressources informatiques, dotées de privilèges plus ou moins élevés, leur permettant de manipuler de l'information au travers d'applications gérés par le SI.

Les usagers du SI sont tenus de lire, d'accepter et d'appliquer les règles relatives à la sécurité du SI, comme la charte de bon usage des moyens informatiques.

Tout usager du système d'information doit être identifié et répertorié dans le carnet de sécurité du SI.

2.10. Organiser des audits réguliers sur la sécurité du SI :

Bien que prévu dans la PSSI, des interventions d'audits doivent être planifiées afin d'établir le niveau de maturité de notre SI, mais certains audits pourront et devront être effectuées auprès des usagers afin de déterminer le respect des différentes règles de sécurité, leur niveau de sensibilisation à la sécurité du SI, ainsi que la détection éventuelle de failles qui ne seraient pas couvertes par l'analyse de risques.

2.11. Sensibilisation à la sécurité :

Les dispositifs de sécurité ne peuvent être efficients que s'ils sont perçus comme des bénéfices et non vécus comme des contraintes.

Pour cela, un apprentissage minimal de la SSI d'ensemble est nécessaire. Divers moyens doivent être utilisés pour y parvenir à savoir : les formations, les séminaires, etc.

2.12. Mise en place d'un PRA :

Un des dispositifs centraux pour la sécurité du SI, est la mise en place d'un Plan de Reprise d'activité à minima. Cette procédure repose avant tout sur la bonne santé du SI en général ainsi que sur la solidité du système de sauvegarde.

Cette procédure vise avant tout à minimiser les risques de perte de disponibilité des différents services du SI, assurer leur confidentialité ainsi que leur intégrité.

Un travail de gestion des risques et d'études des différentes menaces est donc à faire avant la mise en place de cette procédure, notamment au travers d'un Plan d'Action Sécurité.

2.13. Outils de suivi et de reporting :

L'idée étant de pouvoir sortir des indicateurs (KPI, tableaux de bord) quant à l'utilisation du réseau en interne et en externe, ainsi que les différents services informatiques qui sont le plus sollicités.

Ces outils n'ont pour vocation que de mesurer les différentes pointes de trafic, les éventuels engorgements, les services nécessitants plus de ressources, ressortir les différentes périodes d'activités, etc.

Références bibliographiques :

- L. Bloch & C. Wolfhugel "Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs" Eyrolles 2ème édition 2013.
- A. Fernandez Toro "Sécurité opérationnelle –Conseils pratiques pour sécuriser le SI" EYROLLES 2015.
- « Schéma Stratégique Des Systèmes D'information Et Des Télécommunications » S3IT 2008 , Feuille de route 2008-2009 pour la recherche et l'enseignement supérieur https://www.enseignementsup-recherche.gouv.fr/fr
- « Schéma Directeur de la Sécurité du Système d'Information » Université de La Réunion Octobre 2011 .
- « Schéma directeur de la sécurité des systèmes d'information organisation et orientation de la sécurité des systèmes d'information pour les communautés éducatives » ministère de l'Éducation, de l'Enseignement supérieur et de la Recherche de France (mars 2005).
- https://pgccouncil.us/206/Plan-Preparation:
- https://www.designingbuildings.co.uk/wiki/Masterplanning
- « Présentation du Schéma Directeur du Système d'Information » Conseil d'administration de l'université de Bourgogne (25/09/2013).
- https://methodes.pressbooks.com/chapter/schema-directeur/

Annexe :

Résumé du schéma directeur du SI de l'Université de Bourgogne :

Document final approuvé le 03/12/2012

SDSI : période du 2012-2016

Rédigé dans 280 pages : détaillant l'état des lieux du SI, des infrastructures de l'université, et les objectifs d'évolution et de développement.

Quatre objectifs principaux :

1. Placer les Technologies de l'Information et de la Communication (TIC) au cœur de la stratégie de modernisation de l'université
2. Mettre en place de nouvelles formes d'enseignement et de recherche, développer une logique de ressources pour accompagner les enseignants-chercheurs s'engageant dans la voie de l'e-learning
3. Veiller à la performance des équipes, des équipements, des infrastructures informatiques, en associant la Sécurité des Systèmes d'Information
4. Développer le pilotage et améliorer l'urbanisation du système d'information

Ces 4 objectifs sont déclinés en 20 axes stratégiques,

Ces 20 axes sont ensuite déclinés en 43 projets desquels ont émergés 7 projets majeurs et transversaux comme la création d'un Datacenter, et sans lesquels les autres projets ne pourront pas aboutir.

Présentation générale

4 OBJECTIFS	20 AXES	43 PROJETS
UNIVERSITÉ NUMÉRIQUE 5.1 - Placer les TIC au cœur de la stratégie de modernisation de l'établissement	A - Identité et Authentification	5.1.1 - Services et supports d'authentification
	B - Formation, Scolarité	5.1.2 - Evolution des services numériques de la vie étudiante
	C - Recherche et Innovation	5.1.3 - Cohérence du SI recherche au sein de l'uB et homogénéisation avec le SI recherche de l'uFC
	D - Gestion des ressources humaines	5.1.4 - Mise en place d'un nouvel outil de gestion des ressources humaines
	E - Gestion Financière	5.1.5 - Evolution de SIFAC au sein du SI de l'université
	F - Gestion du Patrimoine	5.1.6 - Mise en place d'un SI intégré pour la gestion du patrimoine immobilier de l'uB
		5.1.7 - Pilotage et optimisation de la gestion patrimoniale de l'immobilier de l'uB
	G - Dématérialisation et modernisation des échanges	5.1.8 - Dématérialisation des échanges, partage de données, gestion électronique de documents (GED)

E-LEARNING / E-CAMPUS 5.2 - Mettre en place de nouvelles formes d'enseignement et de recherche, développer une logique de ressources pour le e-learning	A - Pédagogie numérique	5.2.1 - Développement de dispositifs d'enseignements hybrides
		5.2.2 - Développement de l'offre de formation à distance
		5.2.3 - Bac à sable
		5.2.4 - Etoffer la production de ressources numériques
		5.2.5 - Renforcer la formation et l'accompagnement des acteurs
		5.2.6 - Evolution de la plateforme pédagogique (PLUBEL - passage à Moodle 2.3)
		5.2.7 - Impulser les usages du Podcast
		5.2.8 - Développement des usages pédagogiques de la visioconférence et de web conférence
		5.2.9 - Mettre en place une politique éditoriale pour la diffusion des ressources pédagogiques numériques
	B - Aide à l'insertion professionnelle	5.2.10 - Mise en place d'un ePortfolio
		5.2.11 - Ressources pour l'insertion professionnelle – modules e-learning
		5.2.12 - Plate-forme de visibilité des référentiels compétences des formations
	C - Les TIC au service de la politique documentaire	5.2.13 - Mise en valeur du patrimoine numérique des universités de Bourgogne et de Franche-Comté
		5.2.14 - Portail Biomédical : extension de l'offre documentaire et des services de valorisation
		5.2.15 - Restructuration de deux bibliothèques selon le modèle du learning centre
		5.2.16 - Rapprochement des applications documentaires des universités de Bourgogne et de Franche-Comté
	D - Assurer l'évolution de la puissance pour le calcul intensif	5.2.17 - Multiplier la puissance par 10 tous les 4 ans : approcher 533 Tflops en 2016
	E - e-Campus et mobilité des usagers	5.2.18 - Services numériques en ligne et ENT
		5.2.19 - Développement des usages de la messagerie collaborative pour les personnels et les étudiants
		5.2.20 - Evolution des outils de communication web de l'université
		5.2.21 - Développement des services liés à la carte multi-service étudiants et personnels
		5.2.22 - Développement des services de planning

INFRASTRUCTURE NUMÉRIQUE ET SÉCURITÉ 5.3 - Veiller à la performance des équipes, des équipements, des infrastructures informatiques et de la sécurité	A - Création d'un DataCenter au sein de l'uB	5.3.1 - Création d'un DataCenter et veiller à la performance des installations et au fonctionnement des salles machines
	B - Qualité et continuité du réseau informatique et du réseau régional haut débit	5.3.2 - Rénovation et sécurisation de l'architecture réseau : RUBAN 5
		5.3.3 - Évolution du réseau régional haut débit : RESUBIE III
	C - Infrastructures Serveurs et Postes	5.3.4 - Infrastructure de virtualisation
		5.3.5 - Standardisation du parc de postes de travail et industrialisation de la gestion de parc
	D - Assurer la sécurité des SI	5.3.6 - Définir un cadre pour la mise en œuvre d'une Politique de Sécurité du SI
		5.3.7 - Pilotage de la sécurisation du Système d'Information : mise en conformité avec le RGS
		5.3.8 - Gestion opérationnelle de la sécurité : gestion des incidents et plans de secours
		5.3.9 - Protection des acteurs de l'université : sensibiliser, responsabiliser et protéger les utilisateurs vis-à-vis des risques associés aux usages d'Internet
	E - Archivage et stockage de l'information	5.3.10 - Mise en place d'une architecture de stockage centralisée
E-GOUVERNANCE 5.4 - pilotage et urbanisation du SI	A - Pilotage et autonomie de l'uB	5.4.1 - Pour le pilotage, construction des tableaux de bord communs, Business Object et entrepôts de données
	B - Urbanisation du SI	5.4.2 - Cohérence du SI et des référentiels au sein de l'uB et homogénéisation avec le SI de l'uFC
	C - Schéma directeur du système d'information	5.4.3 - Rédaction et validation du Schéma directeur du SI global et transversal

Parmi ces 43 projets, ces 7 projets sont majeurs et incontournables pour l'avenir de l'université et de son système d'information :

1. Création d'un DataCenter et veiller à la performance des infrastructures
2. Mise en place d'un nouvel outil de gestion des ressources humaines
3. Services et supports d'authentification
4. Rénovation de l'architecture réseau
5. Pilotage et urbanisation du SI
6. Développement des usages numériques dans les activités d'enseignement, de recherche et notamment de calcul, de documentation (SCD) et mise en valeur de tout le patrimoine numérique (indexation et dématérialisation)
7. Mise en œuvre d'une Politique de Sécurité du SI