

Référentiel - BTS SIO (Option SISR)

Le BTS SIO (Service Informatique aux Organisations) Option SISR (Solutions d'Infrastructure Système et Réseau)

Compétences clé

- l'installation, l'intégration, l'administration, la sécurisation des équipements et des services informatiques ;
- l'exploitation, la supervision et la maintenance d'une infrastructure systèmes et réseaux ;
- le choix et la mise en œuvre de solutions d'hébergement ;
- la définition et la configuration des postes clients, des serveurs et des équipements d'interconnexion, leur déploiement et leur maintenance ;
- la gestion des actifs de l'infrastructure ;
- la recherche de réponses adaptées à des besoins d'évolution de l'infrastructure ou à des problèmes liés à la mise à disposition des services informatiques ;
- la résolution des incidents et l'assistance des utilisateurs ;
- le maintien de la qualité des services informatiques ;
- la détection, la réaction et l'investigation suite à un incident de sécurité.

En fonction de la taille de l'organisation cliente, la personne titulaire du diplôme peut également être amenée à participer aux missions suivantes :

- l'étude et la caractérisation de solutions d'évolution ou d'optimisation d'une infrastructure ;
- la prise en charge de la relation avec les fournisseurs et les prestataires informatiques ;
- la mesure des performances d'une infrastructure, des équipements ou des services informatiques.

Matrice des compétences

Activités	Bloc de compétences	Unités
	Bloc 4 - culture générale et expression Communiquer par écrit • appréhender et réaliser un message écrit • respecter les contraintes de la langue écrite • synthétiser des informations : fidélité à la signification des documents, exactitude et précision dans leur compréhension et leur mise en relation, pertinence des choix opérés en fonction du problème posé et de la problématique, cohérence de la production ; • répondre de façon argumentée à une question posée en relation avec les documents proposés en lecture. • Communiquer oralement: s'adapter à la situation: maîtrise des contraintes de temps, de lieu, d'objectifs et d'adaptation au destinataire, choix des moyens d'expression appropriés, prise en compte de l'attitude et des questions du ou des interlocuteurs; organiser un message oral : respect du sujet, structure interne du message.	UNITÉ U1 Culture générale et expression

Bloc 5 - expression et communication en langue anglaise

Niveau B2 du CECRL pour les activités langagières suivantes :

- compréhension de documents écrits ;
- production et interaction écrites ;
- compréhension de l'oral ;
- production et interaction orales.

UNITÉ U2

Expression et communication en langue anglaise

Bloc 6 - Mathématiques pour l'informatique

- Comprendre et résoudre les problèmes mathématiques élémentaires auxquels une personne informaticienne est couramment confrontée (calcul binaire, masque de réseau, opérateurs logiques...)
- Comprendre et manipuler les objets mathématiques fréquemment utilisés en programmation, de manière à pouvoir exploiter informatiquement une solution mathématique préalablement construite
- Résoudre des problèmes numériques nécessitant la mise en œuvre d'algorithmes qu'il s'agit de construire, de mettre en forme et dont on comparera éventuellement les performances

UNITÉ U3

Mathématiques pour l'informatique

Bloc 7 - Culture économique, juridique et managériale

Capacités à :

- analyser des situations auxquelles l'entreprise est confrontée ;
- exploiter une base documentaire économique, juridique ou managériale ;
- proposer des solutions argumentées et mobilisant des notions et les méthodologies économiques, juridiques ou managériales adaptées aux situations proposées ;
- établir un diagnostic (ou une partie de diagnostic) préparant une prise de décision stratégique ;
- exposer ses analyses et ses propositions de manière cohérente et argumentée.

UNITÉ U4

Culture économique juridique et managériale pour l'informatique

Domaine d'activité 1 - Support et mise à disposition de services informatiques

- Gestion du patrimoine informatique
- Réponse aux incidents et aux demandes d'assistance et d'évolution
- Développement de la présence en ligne de l'organisation
- Travail en mode projet
- Mise à disposition des utilisateurs d'un service informatique
- Organisation de son développement professionnel

Bloc 1 - Support et mise à disposition de services informatiques

- Gérer le patrimoine informatique
- Répondre aux incidents et aux demandes d'assistance et d'évolution
- Développer la présence en ligne de l'organisation
- Travailler en mode projet
- Mettre à disposition des utilisateurs un service informatique
- Organiser son développement professionnel

UNITÉ U5

Support et mise à disposition de services informatiques

Domaine d'activité 2 - Option « SISR » : Administration des systèmes et des réseaux • Conception d'une solution d'infrastructure • Installation, test et déploiement d'une solution d'infrastructure réseau • Exploitation, dépannage et supervision d'une solution d'infrastructure réseau	Bloc 2 - Option « SISR » : Administration des systèmes et des réseaux • Concevoir une solution d'infrastructure réseau • Installer, tester et déployer une solution d'infrastructure réseau • Exploiter, dépanner et superviser une solution d'infrastructure réseau	UNITÉ U6 Option « SISR » Administration des systèmes et des réseaux
Domaine d'activité 3 - Option « SISR » : Cybersécurité des services informatiques • Protection des données à caractère personnel • Préservation de l'identité numérique de l'organisation • Sécurisation des équipements et des usages des utilisateurs • Garantie de la disponibilité, de l'intégrité et de la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques • Cybersécurisation d'une infrastructure réseau, d'un système, d'un service	Bloc 3 - Option « SISR » : Cybersécurité des services informatiques • Protéger les données à caractère personnel • Préserver l'identité numérique de l'organisation • Sécuriser les équipements et les usages des utilisateurs • Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques • Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service	UNITÉ U7 Option « SISR » Cybersécurité des services informatiques

	Bloc facultatif - Langue vivante 2 Niveau B1 du CECRL pour les activités langagières suivantes : • compréhension de documents écrits ; • production et interaction écrites ; • compréhension de l'oral ; • production et interaction orales.	UNITÉ FACULTATIVE Langue vivante 2
	Bloc facultatif - Mathématiques approfondies Capacités à : • s'informer sur les outils mathématiques ; • chercher en utilisant les outils mathématiques ; • raisonner et argumenter à l'aide d'outils mathématiques ; • effectuer des calculs relevant des mathématiques approfondies avec une calculatrice et d'autres moyens informatiques ; • modéliser, interpréter et communiquer sur les résultats ainsi obtenus.	UNITÉ FACULTATIVE Mathématiques approfondies
	Bloc facultatif - Parcours de certification complémentaire Construire une démarche personnelle d'acquisition de compétences complémentaires.	UNITÉ FACULTATIVE Parcours de certification complémentaire

Bloc facultatif - Engagement étudiant
Approfondissement des compétences évaluées à l'épreuve E5

Développement de compétences spécifiques à un domaine ou à une activité professionnelle particulière en lien avec le référentiel du diplôme et plus particulièrement s'agissant des compétences évaluées dans l'épreuve E5.

UNITÉ FACULTATIVE
Engagement étudiant

Info : Pour la répartition horaire, consulter : [Ressource - Répartition horaire BTS SIO \(SISR\)](#)

Contenu de la formation

U5 - Support et mise à disposition des systèmes informatiques

En prenant en charge la fonction de support informatique, la personne titulaire du diplôme répond aux attentes des utilisateurs ou des clients en s'assurant de la disponibilité des services existants et de la mise à disposition de nouveaux services. Ainsi, en prenant en compte les besoins métiers de l'organisation, elle accompagne sa transformation numérique tout en maintenant son employabilité.

Pour assurer les missions qui lui sont confiées, la personne titulaire du diplôme est amenée à travailler en mode projet en collaborant avec des membres de l'organisation ou des partenaires.

Conditions de réalisation & résultats attendus

Conditions d'exercice

La personne titulaire du diplôme exerce en tant que :

- Référent informatique dans une petite structure ou médiateur numérique entre organisation cliente et prestataires au sein d'une structure plus importante.
 - Son rôle consiste à apporter un premier niveau de support informatique aux utilisateurs au sein de l'organisation : bon fonctionnement du poste de travail en réseau, disponibilité des logiciels et des applications, réponses aux demandes d'assistance de premier niveau et orientation des autres demandes pour une prise en charge adaptée, déploiement et configuration d'un nouveau service. Elle participe aussi au développement de la présence en ligne de l'organisation et à la mise à disposition de nouveaux services. Au sein d'une petite structure, la personne titulaire du diplôme exerce ses activités en relation directe avec la direction de l'organisation et en étroite collaboration avec des prestataires d'entreprises de services informatiques.
 - Dans ce contexte, elle est capable de réaliser les tâches qui lui sont confiées de façon autonome ou en sollicitant les services d'un prestataire ;
- Membre de la direction des systèmes d'information au sein d'une structure plus importante, comme support auprès des utilisateurs et des clients, ou en tant que médiateur numérique.
 - Dans ce contexte, elle mène à bien ses activités au sein d'une équipe et prend en charge tout ou partie d'une demande d'assistance, de déploiement ou de paramétrage d'un service. La personne titulaire du diplôme prend en compte les évolutions des usages (notamment ceux liés à la mobilité des terminaux) et des services (notamment l'informatique en nuage -cloud computing-).

Ressources et moyens mis à disposition

- Description de l'organisation cliente : son métier, ses processus, ses acteurs, son système d'information et sa politique de communication.
- Description du prestataire informatique et des modalités de gestion du système d'information.
- Description du système informatique (infrastructure de communication, cartographie des applications, règles de sécurité, documentation relative à la continuité et la reprise d'activité).
- Référentiels, normes et méthodes adoptées au sein de l'organisation.
- Réglementation, normes et standards du secteur informatique.

- Besoins exprimés dans un périmètre d'intervention donné, en termes de demande d'assistance, de projet, de mise en place d'un nouveau service, de protection des données à caractère personnel.

Relations

Relations internes

- Direction de l'organisation
- Membres de l'équipe prestataire informatique
- Utilisateurs

Relations externes

- Entreprises de services numérique
- Éditeurs de logiciels
- Fournisseurs de services d'informatique en nuage (cloud)
- Fournisseurs d'équipements informatiques

Résultats attendus

- Patrimoine informatique recensé et actualisé
- Assistance réalisée de manière à garantir la continuité de service
- Présence de l'organisation sur le Web conforme à la politique de communication de l'organisation
- Projet conduit dans le respect des contraintes et contingences, y compris organisationnelles et juridiques
- Service mis à disposition dans le respect des pratiques de l'organisation avec appropriation par les utilisateurs
- Environnement d'apprentissage personnel actualisé
- Identité numérique professionnelle maîtrisée

En termes de comportement et de communication

- Écouter, interpréter et prendre en compte les demandes des utilisateurs et des clients, en autonomie ou en relayant vers une personne ou une entité habilitée et compétente.
- Informer et sensibiliser les utilisateurs et les clients concernant le stockage et le traitement des données à caractère personnel.
- Documenter ses actions.
- Savoir anticiper, gérer des priorités et faire preuve de sang-froid.
- Être capable de collaborer au sein d'une équipe d'informaticiens et d'échanger avec les clients et les partenaires.
- Avoir l'esprit d'initiative et être autonome.
- S'adapter à des situations complexes, sous contraintes.

- Avoir une communication écrite et orale adaptée aux acteurs internes et externes :
 - rendre compte synthétiquement des actions entreprises et des réalisations ;
 - adapter sa communication aux différents types d'interlocuteurs;
 - respecter les règles de confidentialité.
- S'impliquer dans l'actualisation de ses connaissances professionnelles et se former si nécessaire.

A1.1 - Gestion du patrimoine informatique

- Recensement et identification des ressources numériques
- Exploitation des référentiels, normes et standards adoptés par le prestataire informatique
- Mise en place et vérification des niveaux d'habilitation associés à un service
- Vérification des conditions de la continuité d'un service informatique
- Gestion des sauvegardes
- Vérification du respect des règles d'utilisation des ressources numériques

A1.2 - Réponse aux incidents et aux demandes d'assistance et d'évolution

- Collecte, suivi et orientation des demandes
- Traitement des demandes concernant les applicatifs, services réseau et système
- Traitement des demandes concernant les applications

A1.3 - Développement de la présence en ligne de l'organisation

- Participation à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques
- Référencement des services en ligne de l'organisation et mesure de leur visibilité
- Participation à l'évolution d'un site Web exploitant les données de l'organisation

A1.4 - Travail en mode projet

- Analyse des objectifs et des modalités d'organisation d'un projet
- Planification des activités
- Évaluation des indicateurs de suivi d'un projet et analyse des écarts

A1.5 - Mise à disposition des utilisateurs d'un service informatique

- Test d'intégration et d'acceptation d'un service
- Déploiement d'un service
- Accompagnement des utilisateurs dans la mise en place d'un service

A1.6 - Organisation de son développement professionnel

- Mise en place de son environnement d'apprentissage personnel
- Mise en œuvre d'outils et de stratégie veille informationnelle
- Gestion de son identité professionnelle
- Développement de son projet professionnel

U6 - Option A "SISR" : Administration systèmes et réseaux

En prenant en compte les besoins métiers de l'organisation, la personne titulaire du diplôme participe à l'administration des systèmes et du réseau de l'organisation. Elle répond aux attentes des utilisateurs ou des clients en réalisant ou en modifiant des solutions d'infrastructure pour assurer le niveau de disponibilité adapté de ces solutions ainsi que la qualité de service des équipements réseaux.

Les interventions concernent à la fois les équipements réseaux et les services qui s'appuient sur des systèmes, eux-mêmes installés sur des serveurs physiques ou virtuels ; certains de ces éléments pouvant être accessibles dans le réseau local ou à travers une solution en nuage (cloud).

Condition de réalisation & résultats attendus

Conditions d'exercice

La personne titulaire du diplôme participe à l'administration du réseau, des serveurs, des systèmes et des services en réalisant ou en modifiant des solutions d'infrastructure et en

assurant le niveau de disponibilité adapté de ces solutions ainsi que la qualité de service des équipements réseaux. Elle prend en compte les évolutions des usages (notamment ceux liés à la mobilité des terminaux) et des services (notamment l'informatique en nuage -cloud computing-).

Ressources et moyens mis à disposition

- Description de l'organisation : son métier, ses processus, ses acteurs et son système d'information.
- Description du prestataire informatique et des modalités de gestion du système d'information.
- Description du système informatique.
- Référentiels, normes et méthodes adoptés au sein de l'organisation.
- Réglementation, normes et standards du secteur informatique.
- Contrat de prestations de services.
- Environnement de production opérationnel.
- Cahier des charges fourni par l'organisation cliente (avec les spécifications fonctionnelles et éventuellement techniques du service à concevoir).

Relations

Relations internes

- Direction de l'organisation
- Membres de l'équipe prestataire informatique
- Utilisateurs

Relations externes

- Entreprises de services numérique
- Éditeurs de logiciels
- Fournisseurs de services d'informatique en nuage (cloud)
- Fournisseurs d'équipements informatiques

Résultats attendus

- Solution d'infrastructure proposée dont les spécifications sont conformes au cahier des charges
- Solution d'infrastructure opérationnelle conformément aux spécifications
- Documentation produite conformément aux règles applicables et référentiels en vigueur chez le prestataire informatique ou l'organisation cliente
- Solution d'infrastructure supervisée et maintenue en condition opérationnelle

En termes de comportement et de communication

- Savoir anticiper, gérer des priorités et faire preuve de sang-froid.
- Être capable de collaborer au sein d'une équipe d'informaticiens et d'échanger avec les utilisateurs, les clients et les partenaires.
- Avoir l'esprit d'initiative et être autonome dans ses actions.
- S'adapter à des situations complexes, sous contraintes.
- Avoir une communication écrite et orale adaptée aux acteurs internes et externes :
 - rendre compte synthétiquement des actions entreprises et des réalisations ;
 - adapter sa communication aux différents types d'interlocuteurs ;
 - respecter les règles de confidentialité.
- S'impliquer dans l'actualisation de ses connaissances professionnelles et se former si nécessaire.

A2.A1 - Conception d'une solution d'infrastructure

- Analyse d'un besoin exprimé et de son contexte juridique
- Étude de l'impact d'une évolution d'un élément d'infrastructure sur le système informatique
- Élaboration d'un dossier de choix d'une solution d'infrastructure et rédaction des spécifications techniques
- Choix des éléments nécessaires pour assurer la qualité et la disponibilité d'un service
- Maquettage et prototypage d'une solution d'infrastructure permettant d'atteindre la qualité de service attendue
- Détermination et préparation des tests nécessaires à la validation de la solution d'infrastructure retenue

A2.A2 - Installation, test et déploiement d'une solution d'infrastructure réseau

- Installation et configuration d'éléments d'infrastructure
- Installation et configuration des éléments nécessaires pour assurer la continuité des services
- Installation et configuration des éléments nécessaires pour assurer la qualité de service (QoS)
- Rédaction ou mise à jour de la documentation technique et utilisateur d'une solution d'infrastructure
- Test d'intégration et d'acceptation d'une solution d'infrastructure
- Déploiement d'une solution d'infrastructure

A2.A3 - Exploitation, dépannage et supervision d'une solution d'infrastructure réseau

- Administration sur site et à distance des éléments d'une infrastructure
- Automatisation des tâches d'administration
- Gestion des indicateurs et des fichiers d'activité des éléments d'une infrastructure
- Identification, qualification, évaluation et réaction face à un incident ou à un problème
- Évaluation, maintien et amélioration de la qualité d'un service

U7 - Cybersécurité des services informatiques

La sécurité des services informatiques constitue un enjeu économique important.

La personne titulaire du diplôme participe à la mise en œuvre d'une politique de cybersécurité définie par le prestataire informatique et à son intégration dans la politique de sécurité de l'organisation.

En lien avec les besoins métiers de l'organisation et de sa transformation numérique, il s'agit de répondre à l'exigence de sécurité du système d'information en prenant en compte toutes ses dimensions (technique, organisationnelle, humaine, juridique, réglementaire).

En fonction de la spécialité du diplôme, la personne titulaire participe à la sécurité des solutions d'infrastructure ou à la sécurité des solutions applicatives et de leur développement.

Conditions de réalisation & résultats attendus

Conditions d'exercice

La personne titulaire du diplôme participe à la mise en œuvre de la politique de sécurité de l'organisation en prenant en compte les enjeux éthiques et déontologiques.

Elle contribue à la protection des données de l'organisation, à la sensibilisation des utilisateurs aux usages et à la sécurisation de leurs accès aux services informatiques.

Elle applique les procédures d'exploitation de sécurité, apportant ainsi son soutien aux opérations d'audit et de contrôle.

En fonction de sa spécialité, elle est en mesure :

- de déployer et d'administrer des solutions de gestion de la sécurité, ainsi que de paramétrer les éléments de sécurité des équipements des serveurs, des services et des terminaux traitants ;
- d'appliquer les recommandations de sécurité dans le développement d'une application informatique.

Elle participe à la détection, à l'investigation et à la réponse aux incidents de sécurité dans son domaine d'expertise.

Ressources et moyens mis à disposition

- Description de l'organisation : son métier, ses processus, ses acteurs et son système d'information.
- Description du prestataire informatique et des modalités de gestion du système d'information.
- Description du système informatique.
- Référentiels, normes et méthodes adoptés au sein de l'organisation.
- Réglementation, normes et standards du secteur informatique.
- Contrat de prestation de service.
- Environnement de production opérationnel.
- Cahier des charges fourni par l'organisation cliente (avec les spécifications fonctionnelles et éventuellement techniques du service à concevoir).
- Logiciel de gestion d'incidents.

Relations

Relations internes

- Direction de l'organisation
- Membres de l'équipe
- prestataire informatique
- Utilisateurs
- Fraudeurs internes

Relations externes

- Organisation cliente
- Entreprises de services numérique
- Éditeurs de logiciels
- Fournisseurs de services d'informatique en nuage (cloud)
- Fournisseurs d'équipements informatiques
- Organisations en charge de la sécurité des systèmes d'information
- Police et justice
- Fraudeurs externes

Résultats attendus

- Application des règles déontologiques participant à la sécurité et des chartes en vigueur.
- Respect de la législation en vigueur concernant la protection des données à caractère personnel.
- Utilisateurs sensibilisés à la politique de sécurité.
- Politique de sécurité de l'organisation respectée en matière de protection :
 - des données à caractère personnel et des données de l'organisation ;
 - des identités numériques ;
 - des ressources numériques ;
 - des accès utilisateurs.
- Gestion des incidents de sécurité dans les délais. Selon la spécialité :
 - les solutions d'infrastructure systèmes services et réseaux sont sécurisées ;
 - les solutions applicatives et leur développement sont sécurisés.

En termes de comportement et de communication

- Savoir anticiper, gérer des priorités et faire preuve de sang-froid.
- Être capable de collaborer au sein d'une équipe d'informaticiens et d'échanger avec les utilisateurs, les clients et les partenaires.
- Avoir l'esprit d'initiative et être autonome dans ses actions.
- S'adapter à des situations complexes, sous contraintes.
- Avoir une communication écrite et orale adaptée avec les acteurs internes et externes :
 - rendre compte synthétiquement des actions entreprises et des réalisations ;
 - adapter sa communication aux différents types d'interlocuteurs ;
 - respecter les règles de confidentialité.
- S'impliquer dans l'actualisation de ses connaissances professionnelles et se former si nécessaire.
- Savoir transférer la gestion des risques à un tiers de confiance (assurance, sous-traitance).

A3.1 - Protection des données à caractère personnel

- Recensement des traitements sur les données à caractère personnel au sein de l'organisation
- Identification des risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel
- Application de la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel
- Sensibilisation des utilisateurs à la protection des données à caractère personnel

A3.2 - Préservation de l'identité numérique de l'organisation

- Protection de l'identité numérique d'une organisation
- Déploiement de moyens appropriés de preuve électronique

A3.3 - Sécurisation des équipements et des usages des utilisateurs

- Information des utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promotion des bons usages à adopter
- Identification des menaces et mise en œuvre des défenses appropriées
- Gestion des accès et des privilèges appropriés
- Vérification de l'efficacité de la protection

A3.4 - Garantie de la disponibilité, de l'intégrité et de la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

- Caractérisation des risques liés à l'utilisation malveillante d'un service informatique
- Recensement des conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité
- Identification des obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation
- Organisation de la collecte et de la conservation de la preuve électronique
- Application des procédures garantissant le respect des obligations légales

A3.5 - Cybersécurisation d'une infrastructure réseau, d'un système, d'un service

- Vérification des éléments contribuant à la sûreté d'une infrastructure informatique
- Prise en compte de la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure

- Mise en œuvre et vérification de la conformité d'une infrastructure à un référentiel, une norme ou un standard participant à la sécurité
- Prévention des attaques
- Détection des actions malveillantes
- Analyse d'incidents de sécurité, proposition et mise en œuvre de contre-mesures

Compétences

Bloc 1 - Support et mise à disposition des systèmes informatiques

Conditions de réalisation et ressources nécessaires

Contexte

La personne titulaire du diplôme exerce des activités de support et de mise à disposition de services informatiques pour répondre aux besoins d'une organisation cliente. Elle travaille pour le compte de l'entité informatique interne d'une organisation cliente, d'une entreprise de services du numérique, d'une société de conseil en technologies ou encore d'un éditeur de logiciels informatiques.

Les contextes de travail, ouverts et évolutifs, nécessitent de mener une veille informationnelle et technologique et de prendre en compte leurs aspects humains, technologiques, organisationnels, économiques et juridiques.

La personne titulaire du diplôme intervient dans un environnement technologique opérationnel.

Ressources

- Description de l'organisation cliente : son métier, ses processus, ses acteurs (internes et externes), son système d'information et sa politique de communication.

- Description du prestataire informatique : ses compétences, ses méthodes, ses outils, ses procédures et référentiels.
- Description du système informatique de l'organisation cliente : infrastructure de communication, cartographie des applications, règles de sécurité.
- Référentiels, normes, réglementations, chartes, standards et méthodes mobilisées dans le cadre de la mise à disposition d'un service.
- Contrat de prestation de services.
- Environnement de production opérationnel et conforme à l'environnement technologique décrit dans l'annexe II.E du diplôme.
- Cahier des charges (avec les spécifications fonctionnelles et éventuellement techniques du service à mettre à disposition).

Degré d'autonomie, responsabilités

La personne titulaire du diplôme est en charge, pour le compte des utilisateurs et des clients, de tout ou partie du support et de la mise à disposition des services informatiques. Elle travaille dans un périmètre donné en respectant les étapes du processus de prise en compte des demandes d'intervention, ou bien, au sein d'une équipe projet, à la mise à disposition d'un nouveau service. Pour ce faire elle est consciente des enjeux liés à la gestion des actifs informatiques.

Elle écoute et interprète les demandes des utilisateurs et des clients. Elle prend en compte ces demandes, les qualifie et les traite ou les relaie vers une personne ou une entité habilitée et compétente. Elle informe et sensibilise les utilisateurs et les clients concernant le support et la mise à disposition des services informatiques. Elle rend compte de ses activités afin de constituer une documentation (FAQ, banque de connaissances, etc.).

C1.1 - Gérer le patrimoine informatique

Compétences

- Recenser et identifier les ressources numériques
- Exploiter des référentiels, normes et standards adoptés par le prestataire informatique
- Mettre en place et vérifier les niveaux d'habilitation associés à un service
- Vérifier les conditions de la continuité d'un service informatique
- Gérer des sauvegardes
- Vérifier le respect des règles d'utilisation des ressources numériques

Indicateurs de performance

- Le recensement du patrimoine informatique est exhaustif et réalisé au moyen d'un outil de gestion des actifs informatiques.
- Les référentiels, normes et standards sont mobilisés de façon pertinente.
- Les droits mis en place correspondent aux habilitations des acteurs.
- Les conditions de continuité et de reprise d'un service sont vérifiées et les manquements sont signalés.
- Les sauvegardes sont réalisées dans les conditions prévues conformément au plan de sauvegarde.
- Les restaurations sont testées et opérationnelles.
- Les écarts par rapport aux règles d'utilisation des ressources numériques sont détectés et signalés.

Savoirs associés

Savoirs technologiques

- Patrimoine informatique : définition, outils de gestion
- Système informatique
- Système d'exploitation : gestion des utilisateurs, habilitations et droits d'accès
- Disponibilité d'un service informatique : enjeux techniques, économiques et juridiques
- Plans de continuité et de reprise d'activité
- Typologie et techniques de sauvegarde et de restauration
- Typologie des supports de sauvegarde

Savoirs économiques, juridiques et managériaux

- Typologie des acteurs de l'industrie informatique
- Normes et standards : enjeux techniques et économiques
- Typologie des licences logicielles, modalités de tarification
- Gestion des actifs informatiques : méthodes, enjeux techniques, financiers, organisationnels et juridiques pour l'organisation
- Contrat de prestation de service informatique et autres contrats liés à la gestion du patrimoine informatique
- Obligations légales en matière de conservation et d'archivage des données
- Charte informatique et sa valeur juridique
- Responsabilités du salarié utilisateur des ressources informatiques

C1.2 - Répondre aux incidents et aux demandes d'assistance et d'évolution

Compétences

- Collecter, suivre et orienter des demandes
- Traiter des demandes concernant les services réseau et système, applicatifs

- Traiter des demandes concernant les applications

Indicateurs de performance

En utilisant les outils adaptés, les demandes d'assistance ont été prises en compte, correctement diagnostiquées et leur traitement correspond aux attentes.

- La réponse à une demande d'assistance est conforme à la procédure et adaptée à l'utilisateur.
- La méthode de diagnostic de résolution d'un incident est adéquate et efficiente.
- Une solution à l'incident est trouvée et mise en œuvre.
- Le cycle de résolution des demandes respecte les normes et standards du prestataire informatique.
- L'utilisation d'un logiciel de gestion de parc et d'incidents est maîtrisée.
- Le compte rendu d'intervention est clair et explicite.
- La communication écrite et orale est adaptée à l'interlocuteur.

Savoirs associés

Savoirs technologiques

- Outils et méthodes de gestion des incidents
- Méthodologie de repérage de la cause d'un incident, d'une panne
- Base de connaissances d'un centre d'assistance (helpdesk)
- Prise de contrôle d'un poste de travail
- Normes et standards concernant la gestion des configurations et la gestion d'incidents
- Méthodes et outils de diagnostic
- Bases du réseau : modèles de référence, médias d'interconnexion, protocoles de base et services associés, adressage, nommage, routage, principaux composants matériels, notion de périmètres réseau
- Principaux composants matériels des équipements utilisateur et des serveurs
- Système d'exploitation : logiciels des équipements utilisateur et des serveurs, fonctionnalités des systèmes d'exploitation des équipements utilisateur et serveurs, virtualisation
- Bases de la programmation : structures de données et de contrôle, procédures, fonctions, utilisation d'objets
- Langage de commande d'un système d'exploitation : commandes usuelles et script

Savoirs économiques, juridiques et managériaux

- Entente de niveau de service et contrat d'assistance : obligations et responsabilités

C1.3 - Développer la présence en ligne de l'organisation

Compétences

- Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques.
- Référencer les services en ligne de l'organisation et mesurer leur visibilité.
- Participer à l'évolution d'un site Web exploitant les données de l'organisation.

Indicateurs de performance

- L'image de l'organisation est conforme aux attentes et valorisée.
- Les enjeux économiques liés à l'image de l'organisation sont identifiés et les obligations juridiques sont respectées.
- Les mentions légales sont accessibles et conformes à la législation.
- La visibilité des services en ligne de l'organisation est satisfaisante.
- Le site Web a évolué conformément au besoin exprimé

Savoirs associés

Savoirs technologiques

- Référencement et mesure d'audience d'un service en ligne
- Conventions d'écriture électronique
- Charte graphique
- Bases de la programmation Web : langage de présentation et de mise en forme, langage d'accès aux données, langage de contrôle
- Langage d'interrogation de données
- Système de gestion de contenus : fonctionnalités et paramétrage

Savoirs économiques, juridiques et managériaux

- E-réputation d'une organisation : modalités de construction, atteintes, protection juridique et enjeux économiques
- Responsabilité de l'éditeur et de l'hébergeur du site Web
- Mentions légales et conditions générales d'utilisation d'un site Web
- Réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel
- Droit d'utilisation des contenus externes
- Nom de domaine : formalisme, organismes d'attribution et de gestion, conflits et résolution

C1.4 - Travailler en mode projet

Compétences

- Analyser les objectifs et les modalités d'organisation d'un projet
- Planifier les activités
- Évaluer les indicateurs de suivi d'un projet et analyser les écarts

Indicateurs de performance

- Les objectifs et les modalités d'organisation du projet sont explicités.
- L'analyse des besoins et de l'existant est pertinente.
- Les activités personnelles sont planifiées selon une méthodologie donnée et les ressources humaines, matérielles et logicielles nécessaires sont mobilisées de manière efficace et pertinente.
- Le découpage en tâches est réaliste.
- Les livrables sont conformes.
- Le projet est documenté.
- Un compte rendu clair et concis est réalisé et les écarts sont justifiés.
- La communication écrite et orale est adaptée à l'interlocuteur.

Savoirs associés

Savoirs technologiques

- Planification de projet : approche prédictive et séquentielle, approche agile.
- Outil de gestion de projet : fonctionnalités et paramétrage.

Savoirs économiques, juridiques et managériaux

<non précisés>

C1.5 - Mettre à disposition des utilisateurs un service informatique

Compétences

- Réaliser les tests d'intégration et d'acceptation d'un service
- Déployer un service
- Accompagner les utilisateurs dans la mise en place d'un service

Indicateurs de performance

- Des tests pertinents d'intégration et d'acceptation sont rédigés et effectués.
- Les outils de test sont utilisés de manière appropriée.
- Un rapport de test du service est produit.
- Un support d'information est disponible.
- Les modalités d'accompagnement sont définies.
- Le service déployé est opérationnel et donne satisfaction à l'utilisateur.

Savoirs associés

Savoirs technologiques

- Service informatique : prestations, moyens techniques, rôles des parties prenantes
- Principes d'architecture d'un service
- Services et protocoles réseaux standard et de base
- Techniques et outils de déploiement des services informatiques
- Techniques et outils de test des services informatiques

Savoirs économiques, juridiques et managériaux

<non précisé>

C1.6 - Organiser son développement professionnel

Compétences

- Mettre en place son environnement d'apprentissage personnel
- Mettre en œuvre des outils et stratégies de veille informationnelle
- Gérer son identité professionnelle
- Développer son projet professionnel

Indicateurs de performance

- Les besoins de formation sont identifiés pour assurer le support ou mettre à disposition un service.
- L'environnement d'apprentissage personnel est délimité et expliqué.
- La veille est régulière et vise à :
 - repérer les techniques et technologies émergentes du secteur informatique ;
 - d'utiliser de manière approfondie des moyens de recherche d'information ;
 - de renforcer de ses compétences.
- L'identité professionnelle est pertinente et visible sur un réseau social professionnel.

Savoirs associés

Savoirs technologiques

- Gestion des relations professionnelles : identité numérique professionnelle, techniques de rédaction de curriculum vitae et de lettre de motivation, présence sur les réseaux sociaux professionnels (outils, atouts et risques)
- Veille informationnelle et curation : sources d'information, stratégies et outils.
- Panorama des métiers de l'informatique

Bloc 2 - Option A "SISR" : Administration systèmes et réseaux

Conditions de réalisation et ressources nécessaires

Contexte

La personne titulaire du diplôme exerce des activités d'administration des systèmes et des réseaux pour répondre aux besoins d'une organisation cliente. Elle travaille pour le compte de l'entité informatique interne à une organisation cliente, d'une entreprise de services du numérique, d'une société de conseil en technologies ou encore d'un éditeur de logiciels informatiques.

Les contextes de travail, ouverts et évolutifs, nécessitent de mener une veille informationnelle et technologique et de prendre en compte leurs aspects humains, technologiques, organisationnels, économiques et juridiques.

La personne titulaire du diplôme met en œuvre l'environnement technologique nécessaire à l'administration des systèmes et des réseaux : environnement de prototypage ou de tests, outil collaboratif de suivi et de gestion du patrimoine informatique ou encore bases de connaissances.

Ressources

- Description de l'organisation cliente : son métier, ses processus, ses acteurs (internes et externes) et son système d'information.
- Description du prestataire informatique de l'organisation cliente : ses compétences, ses méthodes, ses outils, ses procédures et référentiels.
- Description du système informatique de l'organisation cliente : infrastructure de communication, cartographie des applications, règles de sécurité.

- Référentiels, normes, réglementations, chartes, standards et méthodes mobilisés dans le cadre de la mise en œuvre d'une infrastructure.
- Contrat de prestation de services.
- Environnement de production opérationnel et conforme à l'environnement technologique décrit dans l'annexe II.E.
- Cahier des charges fourni par l'organisation cliente (avec les spécifications fonctionnelles et éventuellement techniques du service à concevoir, à réaliser ou à adapter).

Degré d'autonomie, responsabilités

La personne titulaire du diplôme est en charge de tout ou partie des serveurs et des postes de travail informatiques de l'organisation cliente ainsi que du développement ou de la maintenance de son infrastructure réseau.

Elle travaille dans un périmètre donné en respectant les méthodes, normes et standards qui prévalent au sein de l'organisation cliente. Elle travaille en totale autonomie dans une petite structure cliente ou bien au sein d'une équipe projet.

Sa veille technologique lui permet de choisir les technologies adéquates pour implémenter, les fonctionnalités techniques qui lui ont été confiées, dans le respect de la législation en vigueur et des principes éthiques de la profession. La personne titulaire du diplôme rend compte de ses activités à son responsable ou au client final. Elle assure des activités de formation auprès des utilisateurs et leur fournit une documentation d'utilisation du service développé ou amélioré.

C2.A1 - Concevoir une solution d'infrastructure réseau

Compétences

- Analyser un besoin exprimé et son contexte juridique
- Étudier l'impact d'une évolution d'un élément d'infrastructure sur le système informatique
- Élaborer un dossier de choix d'une solution d'infrastructure et rédiger les spécifications techniques
- Choisir les éléments nécessaires pour assurer la qualité et la disponibilité d'un service
- Maquetter et prototyper une solution d'infrastructure permettant d'atteindre la qualité de service attendue
- Déterminer et préparer les tests nécessaires à la validation de la solution d'infrastructure retenue

Indicateurs de performance

- Les fonctionnalités et les exigences liées à la qualité attendue de la solution d'infrastructure sont identifiées.
- Les contextes d'utilisation, les processus et les acteurs sur lesquels la solution d'infrastructure à produire aura un impact sont décrits.
- Les composants de l'architecture technique sur lesquels la solution d'infrastructure à produire aura un impact sont recensés.
- Les risques liés à une mauvaise utilisation ou à un dysfonctionnement de la solution d'infrastructure sont identifiés.
- Les choix de solutions répondant au besoin exprimé (adaptation d'une solution existante ou réalisation d'une nouvelle) sont décrits et justifiés en termes de coût, de délai et de qualité.
- La solution proposée tient compte des limites de responsabilité du prestataire informatique vis-à-vis de son métier et de son environnement.
- Le dossier de choix et l'argumentaire technique sont rédigés et prennent en compte des préoccupations éthiques et environnementales.
- Les éléments permettant d'assurer la qualité et la continuité des services sont justifiés et caractérisés :
 - les éléments à sauvegarder et à journaliser pour assurer la continuité du service et la traçabilité des transactions sont identifiés ;
 - les procédures d'alerte associées au service sont spécifiées ;
 - les solutions de fonctionnement en mode dégradé et les procédures de reprise du service sont décrites.
- La maquette et le prototype sont conformes au besoin exprimé.
- Les tests d'acceptation nécessaires à la validation de la solution d'infrastructure sont recensés.
- Les jeux d'essai pertinents et les procédures pour la réalisation des tests sont préparés.

Savoirs associés

Savoirs technologiques

- Principes avancés d'architecture des infrastructures réseaux : principes, protocoles, composants, modèles de référence, normes et technologies, plan d'adressage et de nommage, routage, filtrage, périmètres de réseau, services à l'utilisateur, services système et services réseau, virtualisation
- Cahier des charges techniques et formalismes usuels de représentation d'une architecture technique.
- Disponibilité des services, des systèmes, des serveurs et des infrastructures réseaux : méthodes, technologies, techniques, normes et standards associés
- Qualité de service : méthodes, technologies, techniques, normes et standards associés

- Langage de commande d'un système d'exploitation : commandes et script d'administration d'une solution d'infrastructure
- Outil de conception et de simulation d'architecture réseau : techniques, fonctionnalités et paramétrage
- Composition du coût de possession d'une solution d'infrastructure
- Déploiement d'éléments d'infrastructure : méthodes, technologies, techniques, normes et standards associés
- Supervision et métrologie des infrastructures réseaux : méthodes, technologies, techniques, normes et standards associés
- Plans de continuité et de reprise d'activité
- Sauvegarde et restauration : stratégies, techniques, typologie des supports de sauvegarde et technologies associées
- Techniques et outils de test des services informatiques
- Techniques, outils et protocoles d'administration à distance
- Technologie, techniques, normes et standards, outils et méthodes associés au diagnostic et à la gestion des incidents et des problèmes
- Techniques de rédaction d'un compte rendu, d'un argumentaire technique, d'une documentation utilisateur et technique, d'une procédure d'installation et de configuration

Savoirs économiques, juridiques et managériaux

- Contraintes éthiques et environnementales dans le choix d'une solution d'infrastructure réseau
- Cahier des charges et ses enjeux juridiques.
- Contrat de prestation de services informatiques (formation, exécution, inexécution) et ses clauses spécifiques
- Responsabilité civile et pénale de l'administrateur système et réseau

C2.A2 - Installer, tester et déployer une solution d'infrastructure réseau

Compétences

- Installer et configurer des éléments d'infrastructure
- Installer et configurer des éléments nécessaires pour assurer la continuité des services
- Installer et configurer des éléments nécessaires pour assurer la qualité de service
- Rédiger ou mettre à jour la documentation technique et utilisateur d'une solution d'infrastructure
- Tester l'intégration et l'acceptation d'une solution d'infrastructure
- Déployer une solution d'infrastructure

Indicateurs de performance

- Des éléments d'infrastructure (élément d'interconnexion, service, serveur, équipement utilisateur) sont installés et configurés.
- Les éléments d'infrastructure permettant d'assurer la continuité de service sont installés et configurés.
- Le service fonctionne avec la disponibilité attendue.
- Une procédure de remplacement ou de migration d'un élément d'infrastructure est élaborée et mise en œuvre en respectant la continuité d'un service.
- Les éléments d'infrastructure permettant d'assurer la qualité de service sont installés et configurés.
- Le service fonctionne avec la qualité attendue.
- La solution d'infrastructure est installée et configurée dans les règles de l'art :
 - l'environnement de test est mis en place ;
 - les tests pertinents d'intégration et d'acceptation sont effectués ;
 - le rapport de tests est rédigé ;
 - la documentation est à jour et disponible ;
 - la solution d'infrastructure tient compte des préoccupations de développement durable.
- L'intégration de la solution ne génère pas de dysfonctionnement du réseau ou dans le réseau.
- Une procédure claire de déploiement de la solution est rédigée.
- La solution d'infrastructure est déployée selon la procédure et la planification définies.

Savoirs associés

<voir C2.A1>

C2.A3 - Exploiter, dépanner et superviser une solution d'infrastructure réseau

Compétences

- Administrer sur site et à distance des éléments d'une infrastructure
- Automatiser des tâches d'administration
- Gérer des indicateurs et des fichiers d'activité des éléments d'une infrastructure
- Identifier, qualifier, évaluer et réagir face à un incident ou à un problème
- Évaluer, maintenir et améliorer la qualité d'un service

Indicateurs de performance

- Un dispositif d'administration sur site et à distance est configuré et exploité.
- Les conditions d'administration des éléments d'infrastructure sont maîtrisées.
- L'automatisation des tâches d'administration répond au besoin exprimé.
- Les outils nécessaires à la production d'indicateurs d'activité et à l'exploitation de fichiers d'activité sont installés et configurés.

- Les dysfonctionnements récurrents dans une solution d'infrastructure sont repérés et leurs causes identifiées.
- Le degré d'urgence et le niveau d'intervention sont définis.
- Les conséquences techniques du problème sont évaluées.
- L'incident est résolu ou escaladé de manière efficiente, en tenant compte des délais et procédures en vigueur.
- Le problème est résolu ou escaladé de manière efficiente, en tenant compte des délais et procédures en vigueur.
- Les rapports d'incidents et les comptes rendus de problèmes sont rédigés et adaptés à chaque destinataire tant par leur contenu que par leur présentation.
- Des mesures correctives sont proposées ou mises en œuvre pour maintenir ou améliorer la qualité d'un service.
- Les éléments d'une solution d'infrastructure et leur utilisation sont supervisés.
- Les indicateurs et les fichiers d'audit sont analysés et exploités.
- Des alertes adaptées à la criticité du service sont générées.
- Les procédures d'alerte destinées à rétablir la qualité du service sont appliquées.
- Le fonctionnement du service en mode dégradé et la disponibilité des éléments d'infrastructure permettant une reprise du service sont périodiquement vérifiés.
- Le rétablissement de la qualité du service est assuré dans les délais prévus.

Savoirs associés

<voir C2.A1>

Bloc 3 - Cybersécurité des services informatiques

Conditions de réalisation et ressources nécessaires

Contexte

La personne titulaire du diplôme exerce des activités pour répondre aux besoins de sécurité des services informatiques d'une organisation cliente notamment au regard du développement des menaces et attaques en provenance du cybermonde et des risques liés aux usages numériques. Elle travaille pour le compte de l'entité informatique interne à une organisation cliente, d'une entreprise de services du numérique, d'une société de conseil en technologies ou encore d'un éditeur de logiciels informatiques.

Les contextes de travail, ouverts et évolutifs, nécessitent de mener une veille informationnelle et technologique et de prendre en compte leurs aspects humains, technologiques, organisationnels, économiques et juridiques.

La personne titulaire du diplôme participe à la mise en œuvre de l'environnement technologique nécessaire à la sécurité des services informatiques.

Ressources

- Description de l'organisation cliente : son métier, le caractère sensible des activités conduites, ses processus, ses acteurs (internes et externes) et son système d'information.
- Description du prestataire informatique de l'organisation cliente : ses compétences, ses méthodes, ses outils, ses procédures et ses référentiels.
- Description du système informatique de l'organisation cliente : infrastructure de communication, cartographie des applications, règles de sécurité et de sûreté.
- Référentiels, normes, réglementations, chartes, standards et méthodes mobilisés dans le cadre de la mise à disposition d'un service sécurisé.
- Contrat de prestation de services.
- Environnement de production opérationnel et conforme à l'environnement technologique décrit dans l'annexe II.E du diplôme.
- Cahier des charges fourni par l'organisation cliente : spécifications fonctionnelles et éventuellement

Degré d'autonomie, responsabilités

La personne titulaire du diplôme participe à la mise en œuvre de la politique de gestion de la sécurité informatique de l'organisation cliente, en veillant à documenter ses actions. Elle travaille dans un périmètre donné en respectant les méthodes, normes et standards qui prévalent au sein de cette organisation.

Elle participe notamment à l'information et à la sensibilisation des utilisateurs aux risques en recommandant les pratiques adaptées. Elle contribue à la sécurisation des accès aux services informatiques : protection des accès aux ressources numériques, aux données, aux équipements et aux applications. En fonction de sa spécialité, elle intervient plus particulièrement sur la sécurité des infrastructures ou des développements d'application.

Dans une petite structure, elle peut travailler en autonomie en tenant compte des risques spécifiques identifiés pour l'organisation cliente. Elle prend en charge l'information, la sensibilisation et la formation des utilisateurs aux questions de sécurité informatique. Dans une structure plus importante, elle travaille au sein d'une équipe en rendant compte de ses activités.

C3.1 - Protéger les données à caractère personnel

Compétences

- Recenser les traitements sur les données à caractère personnel au sein de l'organisation
 - Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel
 - Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel
- Sensibiliser les utilisateurs à la protection des données à caractère personnel

Indicateurs de performance

- La collecte, le traitement et la conservation des données à caractère personnel sont effectués conformément à la réglementation en vigueur.
- La charte informatique contient des dispositions destinées à protéger les données à caractère personnel.
- Des supports de communication pertinents sont accessibles et adaptés aux utilisateurs.
- Le recensement des traitements des données à caractère personnel est exhaustif.
- Des moyens de protection sont mis en place pour garantir la confidentialité et l'intégrité des données à caractère personnel en tenant compte des risques identifiés.

Savoirs associés

Savoirs technologiques

- Typologie des risques et leurs impacts.
- Principes de la sécurité : disponibilité, intégrité, confidentialité, preuve.
- Sécurité et sûreté : périmètre respectif.
- Sécurité des terminaux utilisateurs et de leurs données : principes et outils.
- Authentification, privilèges et habilitations des utilisateurs : principes et techniques.
- Gestion des droits d'accès aux données : principes et techniques.
- Sécurité des communications numériques : rôle des protocoles, segmentation, administration, restriction physique et logique.
- Protection et archivage des données : principes et techniques.
- Chiffrement, authentification et preuve : principes et techniques.
- Sécurité des applications Web : risques, menaces et protocoles.
- Outils de contrôle de la sécurité : plans de secours, traçabilité et audit technique.

Savoirs économiques, juridiques et managériaux

- Les données à caractère personnel : définition, réglementation, rôle de la CNIL.
- L'identité numérique de l'organisation : risques et protection juridique.
- Droit de la preuve électronique.
- La sécurité des équipements personnels des utilisateurs et de leurs usages : prise en compte des nouvelles modalités de travail, rôle de la charte informatique.
- Les risques des cyberattaques pour l'organisation : économique, juridique, atteinte à l'identité de l'entreprise.
- Obligations légales de notification en cas de faille de sécurité.
- Réglementation en matière de lutte contre la fraude informatique : infractions, sanctions.
- Les organisations de lutte contre la cybercriminalité.

C3.2 - Préserver l'identité numérique de l'organisation

Compétences

- Protéger l'identité numérique d'une organisation
- Déployer les moyens appropriés de preuve électronique

Indicateurs de performance

- L'identité numérique de l'organisation est protégée en s'appuyant sur des moyens techniques et juridiques.
- La preuve électronique est déployée de manière sécurisée et dans le respect de la législation.

Savoirs associés

Savoirs technologiques

<voir C3.1>

C3.3 - Sécuriser les équipements et les usages des utilisateurs

Compétences

- Informer les utilisateurs sur les risques associés à l'utilisation d'une ressource numérique et promouvoir les bons usages à adopter
- Identifier les menaces et mettre en œuvre les défenses appropriées
- Gérer les accès et les privilèges appropriés
- Vérifier l'efficacité de la protection

Indicateurs de performance

- Des supports de communication interne sont accessibles aux utilisateurs et adaptés à leurs destinataires.
- Les outils de défense mis en œuvre permettent de prévenir les menaces identifiées :
 - l'accès physique au terminal et à ses données est sécurisé ;
 - les applications installées sont vérifiées par des procédures automatisées et des logiciels de sécurité ;
 - les flux réseaux sont identifiés et sécurisés.
- Les accès et privilèges respectent les règles organisationnelles :
 - les utilisateurs sont authentifiés ;
 - les habilitations sont configurées ;
 - l'accès aux données est contrôlé ;
 - les privilèges sont restreints.
- L'efficacité de la protection mise en œuvre est évaluée.

Savoirs associés

Savoirs technologiques

<voir C3.1>

C3.4 - Garantir la disponibilité, l'intégrité et la confidentialité des services informatiques et des données de l'organisation face à des cyberattaques

Compétences

- Caractériser les risques liés à l'utilisation malveillante d'un service informatique
- Recenser les conséquences d'une perte de disponibilité, d'intégrité ou de confidentialité
- Identifier les obligations légales qui s'imposent en matière d'archivage et de protection des données de l'organisation
- Organiser la collecte et la conservation des preuves numériques
- Appliquer les procédures garantissant le respect des obligations légales

Indicateurs de performance

- Les risques associés à l'utilisation malveillante d'un service informatique sont caractérisés.
- Les conséquences des actes malveillants sur un service informatique sont identifiées.
- Les obligations légales en matière d'archivage et de protection des données sont identifiées et respectées.
- Les preuves numériques sont conservées de manière sécurisée et dans le respect de la législation.

- Des procédures garantissant le respect des obligations légales sont opérationnelles et appliquées :
 - un schéma présentant la segmentation du réseau est disponible ;
 - les principes de mise en œuvre des contrôles des connexions aux réseaux sont validés ;
 - l'authentification et la confidentialité des échanges sont vérifiées ;
 - la sécurité de l'administration est prise en compte ;
 - les accès physiques et logiques à un serveur ou à un service sont vérifiés en fonction des habilitations et des privilèges définis ;
 - les accès aux données sont contrôlés à chaque étape d'une transaction ;
 - les systèmes et les applications sont actualisés en fonction des alertes de sécurité ;
 - les vulnérabilités connues sont contrôlées

Savoirs associés

Savoirs technologiques

<voir C3.1>

C3.5 - Assurer la cybersécurité d'une infrastructure réseau, d'un système, d'un service

Compétences

- Participer à la vérification des éléments contribuant à la sûreté d'une infrastructure informatique
- Prendre en compte la sécurité dans un projet de mise en œuvre d'une solution d'infrastructure
- Mettre en œuvre et vérifier la conformité d'une infrastructure à un référentiel, une norme ou un standard de sécurité
- Prévenir les attaques
- Détecter les actions malveillantes
- Analyser les incidents de sécurité, proposer et mettre en œuvre des contre-mesures

Indicateurs de performance

- Les dispositifs participant à la disponibilité sont validés (les éléments critiques sont résilients, la charge est répartie efficacement, la qualité des services sensibles est assurée).
- Les failles potentielles sont identifiées grâce à une activité de veille sur les vulnérabilités.
- Les bonnes pratiques de sécurité sont prises en compte.
- Les éléments de sécurité de l'architecture sont conformes et documentés.

- Les exigences de sécurité sont prises en compte dans le projet de mise en œuvre d'une solution d'infrastructure.
- Les dispositifs de détection et de protection des attaques sont opérationnels.
- Les processus de résolution d'un incident ou d'un problème sont respectés.
- Le compte rendu d'intervention est clair et explicite.
- Les contre-mesures mises en place corrigent et préviennent les incidents de sécurité
- Les contre-mesures sont documentées de manière à en assurer le suivi.
- La communication écrite et orale est adaptée à l'interlocuteur.

Savoirs associés

Savoirs technologiques

- Sûreté des infrastructures réseaux : bonnes pratiques, normes et standards.
- Cybersécurité : bonnes pratiques, normes et standards.
- Technologies et équipements de la sécurité informatique des infrastructures réseau, systèmes et services.
- Outils de sécurité : prévention et détection des attaques, gestion d'incidents.

Savoirs économiques, juridiques et managériaux

- Responsabilité civile et pénale de l'administrateur système et réseau.