cegid

Déclaration d'applicabilité ISO27001:2013

Version du 06/01/2022
Classification : Public

Modifiée par : Frédérik GAVOIS

ISO27001:2013

		Solution mise en œuvre	Preuves et livrables
4	**Contexte de l'organisation**		
4.1	Compréhension de l'organisation et son conctexte	Périmètre du Système de Management de la sécurité du SaaS (SEPO12)	SELI030 - D.D.A
4.2	Compréhension des besoins et des attentes des parties intéressés		
4.3	Détermination du domaine d'application du système de management de la sécurité de l'information		
4.4	Système de management de la sécurité de l'information		
5	**Leadership**		
5.1	Leadership et engagement	Gestion de la Gouvernance, des rôles et des responsabilités SMSI (SEPS4)	Lettre d'engagement de la Direction
5.2	Politique		CR réunions des structures de la sécurité de l'information
5.3	Rôles, responsabilités et autorités au sein de l'organisation		
6	**Planification**		
6.1	Actions liées aux risques et opportunités	Processus d'Évaluation et de Traitement du Risque (SEPS5)	Résultats Analyse de risques et PTR
6.2	Objectifs de sécurité de l'information et plans pour les atteindre		
7	**Support**		
7.1	Ressources	Sécurité des Ressources Humaines (SEPO9)	Processus et document RH
7.2	Compétence		
7.3	Sensibilisation		
7.4	Communication	Processus Communication du SMSI (SEPO11)	CR Comite de Sécurité
7.5	Information Documentées	Processus de gestion de la documentation (SEPS2)	Processus GED
8	**Fonctionnement**		
8.1	Planification et contrôle opérationnels	Politique de contrôle, surveillance et Amélioration (SEPO17)	CR Comite de Sécurité
8.2	Appreciation des risques de sécurité de l'information	Processus de gestion des risques (SEPS5)	Resultat Analyse de risques et PTR
8.3	Traitement des risques de sécurité de l'information		
9	**Evaluation des performanaces**		
9.1	Surveillance, mesures, analyse et évaluation	Politique de contrôle, surveillance et Amélioration (SEPO17)	CR Comite de Sécurité
9.2	Audit interne	Gestion de la conformité et des audits (SEPO10)	Planification des audits
9.3	Revue de direction	Gestion de la Gouvernance, des rôles et des responsabilités SMSI (SEPS4)	Revue de direction
10	**Amélioration**		
10.1	Non-conformité et actions correctives	Gestion de la conformité et des audits (SEPO10)	Planification des audits
10.2	Amélioration continue	Politique de contrôle, surveillance et amélioration (SEPO17)	CR Comite de Sécurité CR Revue de direction

OL = Obligations légales
OC = Obligations contractuelles
EB = Engagement Business
BP= Bonnes Pratiques
AR = Analyse de Risques

ISO27001:2013 Annexe A

	Exigences		Retenue	OL	OC	EB	BP	AR	Solution mise en œuvre	Preuves et livrables
5	**Politiques de sécurité de l'information**									**SEPO16 - Politique de sécurité de l'information Cegid Cloud Factory**
5.1	**Orientations de la direction en matière de sécurité de l'information**	**Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'organisation**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
5.1.1	Politiques de sécurité de l'information	Il convient de définir un ensemble de politiques en matière de sécurité de l'information qui soit approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.	OUI				X		Une politique de sécurité de l'information a été rédigée Elle est révisée annuellement et approuvée par la Direction des services Cloud	Lettre d'engagement de la Direction
5.1.2	Revue des politiques de sécurité de l'information	Pour garantir la constance de la pertinence, de l'adéquation et de l'efficacité des politiques liées à la sécurité de l'information, il convient de revoir ces politiques à intervalles programmés ou en cas de changements majeurs.	OUI				X			
6	**Organisation de la sécurité de l'information**									**SEPS4 - Gestion de la Gouvernance, des rôles et des responsabilités SMSI**
6.1	**Organisation interne**	**Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'organisation**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
6.1.1	Fonctions et responsabilités liées à la sécurité de l'information	Il convient de définir et d'attribuer toutes les responsabilités en matière de sécurité de l'information.	OUI				X		L'Equipe sécurité groupe est organisée de manière transverse. Elle est indépendante hiérarchiquement et opérationnellement des activités du SMSI	Présentation des missions et de l'organisation des équipes dédiées à la sécurité de l'information
6.1.2	Séparation des tâches	Il convient de séparer les tâches et les domaines de responsabilité incompatibles pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.	OUI				X		Organisation de type DevOps des missions et des équipes	Organisation des équipes AzurDevOps (Teams)
6.1.3	Relations avec les autorités	Il convient d'entretenir des relations appropriées avec les autorités compétentes.	OUI		X		X		L'équipe Sécurité de Cegid entretien des échanges réguliers avec la CNIL et l'ANSSI	Echange de Mail/Courrier
6.1.4	Relations avec des groupes de travail spécialisés	Il convient d'entretenir des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles.	OUI				X		Les collaborateurs de l'équipe Sécurité de Cegid sont membre des associations suivantes: CLUSIR/CLUSIF/Club ISO27001	Justification des abonnement au Clusir/Clusif/
6.1.5	La sécurité de l'information dans la gestion de projet	Il convient de traiter la sécurité de l'information dans la gestion de projet, quel que soit le type de projet concerné.	OUI				X		Organisation des équipes et des processus en mode agile (AzureDevOps) pour la prise en compte de la sécurité dans les infrastructures et le développement dans tous les projets liés au SMSI	Organisation des équipes AzurDevOps (Teams) Charte de développement sécurisé Convention de services interne Cloud/Dev Sécurité des projets infra
6.2	**Appareils mobiles et télétravail**	**Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		**SEOP7- Politique en matière d'appareils mobiles et télétravail**
6.2.1	Politique en matière d'appareils mobiles	Il convient d'adopter une politique et des mesures de sécurité complémentaires pour gérer les risques découlant de l'utilisation des appareils mobiles	OUI				X	X	Chiffrement des disques des laptops des collaborateurs	

6.2.2	Télétravail	Il convient de mettre en œuvre une politique et des mesures de sécurité complémentaires pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail.	OUI			X		X	Filtres de confidentialité MFA et VPN en situation de mobilité		
7	**Sécurité des ressources humaines**										**SEPO9-Sécurité des Ressources Humaines**
7.1	**Avant l'embauche**	**S'assurer que les salariés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			
7.1.1	Sélection des candidats	Il convient que des vérifications des informations concernant tous les candidats à l'embauche soient réalisées conformément aux lois, aux règlements et à l'éthique, et il convient qu'elles soient proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés	OUI			X			Un contôle des références (Diplômes, extrait de casier judiciare ...) est effectué par le service de recrutement du Groupe		Procédures de recrutement RH Groupe Convention de services SaaS/RH
7.1.2	Termes et conditions d'embauche	Il convient que les accords contractuels conclus avec les salariés et les contractants déterminent leurs responsabilités et celles de l'organisation en matière de sécurité de l'information	OUI			X			Le contrat de travail signé par les nouveaux salariés comporte une clause de confidentilaité et une clause de non concurrence		
7.2	**Pendant la durée du contrat**	**S'assurer que les salariés et les contractants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			
7.2.1	Responsabilités de la direction	Il convient que la direction demande à tous les salariés et contractants d'appliquer les règles de sécurité conformément aux politiques et aux procédures en vigueur dans l'organisation.	OUI				X		Engagement formel de la Direction des services Cloud au travers des différens comités , réunions et communications autours de la sécurité et du SMSI		Lettre d'engagement de la Direction
7.2.2	Sensibilisation, apprentissage et formation à la sécurité de l'information	Il convient que l'ensemble des salariés de l'organisation et, le cas échéant, les contractants suivent un apprentissage et des formations de sensibilisation adaptés et qu'ils reçoivent régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.	OUI			X	X		Une formation sécurité nouveaux collaborateurs est systématiquement dispensée Un plan annuel de sensibilisation est élaboré		Plans de formations et contenus Contenu des sensibilisations et résultats
7.2.3	Processus disciplinaire	Il convient qu'il existe un processus disciplinaire formel et connu de tous pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information.	OUI			X	X		Un processus disciplinaire peut être engagé en cas de manquement à la PSSI ou à la charte d'utilisation des outils et des matériels informatiques		Règlement Intérieur Contrat de travail Clause de confidentilité renforcée
7.3	**Rupture, terme ou modification du contrat de travail**	**Protéger les intérêts de l'organisation dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			
7.3.1	Achèvement ou modification des responsabilités associées au contrat de travail	Il convient de définir les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, d'en informer le salarié ou le contractant et de veiller à leur application.	OUI	X	X				Le collaborateur est informé de ses responsabilités en cas de modification de rupture ou de fin de contrat par son correspondant RH		Contrat de travail
8	**Gestion des actifs**										**SEPO5-Gestion des actifs**
8.1	**Responsabilités relatives aux actifs**	**Identifier les actifs de l'organisation et définir les responsabilités appropriées en matière de protection**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			
8.1.1	Inventaire des actifs	Il convient d'identifier les actifs associés à l'information et aux moyens de traitement de l'information et de dresser et tenir à jour un inventaire de ces actifs.	OUI				X	X	L'inventaire des actifs est revu et mis à jour dans l'outil d'analyse de risques		Liste des actifs
8.1.2	Propriété des actifs	Il convient que les actifs figurant à l'inventaire aient un propriétaire.	OUI				X		Les actifs sont propriétés de la Direction des services Cloud		définir le propriétaire des actifs matériels et le rôle du propriétaire
8.1.3	Utilisation correcte des actifs	Il convient d'identifier, de documenter et de mettre en œuvre des règles d'utilisation correcte de l'information, des actifs associés à l'information et des moyens de traitement de l'information.	OUI		X		X		Une charte d'utilisation des outils informatiques à destination des collaborateurs a été rédigée et communiquée		Charte d'utilsation des outils infomatique
8.1.4	Restitution des actifs	Il convient que tous les salariés et utilisateurs tiers restituent la totalité des actifs de l'organisation qu'ils ont en leur possession au terme de la période d'emploi, du contrat ou de l'accord.	OUI		X		X		Restitution des actifs suivant l'inventaire de la fiche de départ collaborateur sous la responsabilité du manager		Fiche de départ Ressources Humaines Groupe Cegid
8.2	**Classification de l'information**	**S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			**SEPS2-Gestion de la documentation**
8.2.1	Classification des informations	Il convient de classer les informations en termes de valeur, d'exigences légales, de sensibilité ou de leur caractère critique pour l'entreprise.	OUI				X		Les informations sont classifiés suivant 5 critéres		
8.2.2	Marquage des informations	Il convient d'élaborer et de mettre en œuvre un ensemble approprié de procédures pour le marquage de l'information, conformément au plan de classification de l'information adopté par l'organisation	OUI				X		L'ensemble des actifs (documentaires , actifs clients) est soumis à la politique de gestion des actifs. Cette politique prend en compte le niveau de claisssfication des actifs associé à son niveau de diffusion et de chiffrement nécessaire à sa diffusion		RCNT7- Cycle de vie disque client
8.2.3	Manipulation des actifs	Il convient d'élaborer et de mettre en œuvre des procédures de traitement des actifs, conformément au plan de classification de l'information adopté par l'organisation.	OUI				X				
8.3	**Manipulation des supports**	**Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l'information de l'organisation stockée sur des supports.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			
8.3.1	Gestion des supports amovibles	Il convient de mettre en œuvre des procédures de gestion des supports amovibles conformément au plan de classification adopté par l'organisation.	OUI			X			Restriction d'utilsation des médias amovibles (USB) pour les collaborateurs Procédure fournisseur DC pour les média amovibles de stockage des données clients		Charte d'utilisation des outils du SI
8.3.2	Mise au rebut des supports	Il convient de procéder à une mise au rebut sécurisée des supports qui ne servent plus, en suivant des procédures formelles.	OUI	X	X	X			Formatage bas niveau des medias de stockage des postes collaborateurs Destruction physque des médias de stockage données client par les fournisseurs DC		Preuves Destruction des Données par la production SaaS /mise à dsipo de broyeur
8.3.3	Transfert physique des supports	Il convient de protéger les supports contenant de l'information contre les accès non autorisés, l'utilisation frauduleuse ou l'altération lors du transport.	OUI		X	X		X	Chiffrement des médias de stockages amovibles en cas de transfert de données client Suivi des réceptions et des expéditions par Chronopost		RCNT7- Cycle de vie disque client
9	**Contrôle d'accès**										**SEPO1-Contôle des accès**
9.1	**Exigences métier en matière de contrôle d'accès**	**Limiter l'accès à l'information et aux moyens de traitement de l'information**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			

9.1.1	Politique de contrôle d'accès	Il convient d'établir, de documenter et de revoir une politique du contrôle d'accès sur la base des exigences métier et de sécurité de l'information.	OUI		X		X	X		Politique de contrôle des accès revue annuellement	
9.1.2	Accès aux réseaux et aux services en réseau	Il convient que les utilisateurs aient uniquement accès au réseau et aux services en réseau pour lesquels ils ont spécifiquement reçu une autorisation.	OUI				X	X		Une matrice des droits assure la gestion des droits utilisateurs et l'accès aux ressources Cette matrice est révisée annuellement à minima	Matrice des droits
9.2	**Gestion de l'accès utilisateur**	**Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			
9.2.1	Enregistrement et désinscription des utilisateurs	Il convient de mettre en œuvre une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à permettre l'attribution de droits d'accès.	OUI	X	X	X	X	X		Gestion des inscriptions/désinscriptions des utilisateurs dans notre outil d'orchestration de la plateforme Cloud Factory	Service Request et Workflow stratus
9.2.2	Distribution de l'accès aux utilisateurs	Il convient de mettre en œuvre un processus formel de maîtrise de la gestion des accès utilisateur pour attribuer ou révoquer des droits d'accès à tous les types d'utilisateurs de tous les systèmes et de tous les services d'information.	OUI	X	X	X	X	X			
9.2.3	Gestion des privilèges d'accès	Il convient de restreindre et de contrôler l'attribution et l'utilisation des privilèges d'accès.	OUI			X	X	X		Affectation des droits par groupe d'utilsateurs sur les applications à utiliser	Matrice des droits Cegid Cloud Factory
9.2.4	Gestion des informations secrètes d'authentification des utilisateurs	Il convient que l'attribution des informations secrètes d'authentification soit réalisée dans le cadre d'un processus de gestion formel.	OUI			X	X	X		Les informations d'authentification sont communiquées suivant un processus RH formalisé Elles ne sont communiquées qu'a l'attribution du matricule du collaborateur	
9.2.5	Revue des droits d'accès utilisateur	Il convient que les propriétaires d'actifs revoient les droits d'accès des utilisateurs à intervalles réguliers	OUI			X	X	X		Une revalidation des droits des équipes par les manager est effectuée tous les trimestres	Liste de revalidation des droits trimestrielle vlaidée par les manager
9.2.6	Suppression ou adaptation des droits d'accès	Il convient que les droits d'accès de l'ensemble des salariés et utilisateurs tiers à l'information et aux moyens de traitement de l'information soient supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord.	OUI			X	X	X		A la réception de la confirmation de nos outils RH de la fin de la période d'emploi , la demande est traitéedans notre outil d'orchestration.	Service Request et Workflow stratus
9.3	**Responsabilités des utilisateurs**	**Rendre les utilisateurs responsables de la protection de leurs informations d'authentification.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			
9.3.1	Utilisation d'informations secrètes d'authentification	Il convient d'exiger des utilisateurs des informations secrètes d'authentification qu'ils appliquent les pratiques de l'organisation en la matière	OUI			X	X			Des régles d'utilisation des informations secrètes sont clairement définis dans la charte d'utilisation des outils informatique	SENT14- Politique de gestion des mots de passe Charte d'utilisation des outils informatiques
9.4	**Contrôle de l'accès au système et à l'information**	**Empêcher les accès non autorisés aux systèmes et aux applications**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			
9.4.1	Restriction d'accès à l'information	Il convient de restreindre l'accès à l'information et aux fonctions d'application système conformément à la politique de contrôle d'accès.	OUI			X	X			La matrice des droits et des accès définit les accès par groupe de métiers et par application	Matrice des droits
9.4.2	Sécuriser les procédures de connexion	Lorsque la politique de contrôle d'accès l'exige, il convient que l'accès aux systèmes et aux applications soit contrôlé par une procédure de connexion sécurisée.	OUI				X	X		La connexion des collaborateurs de Cegid Cloud Factory aux environnements de production est effectué via un P.A.M (Bastion) et par un système sécurisé d'accès à distance (RDM)	Manuel d'utilisation du PAM
9.4.3	Système de gestion des mots de passe	Il convient que les systèmes qui gèrent les mots de passe soient interactifs et fournissent des mots de passe de qualité.	OUI				X			Une politiques de gestion des mots de passe est définie pour les collaborateurs de Cegid Cloud Factory ainsi que pour les clients utilsateurs des applications Cegid SaaS	SENT14- Politique de gestion des mots de passe
9.4.4	Utilisation de programmes utilitaires à privilèges	Il convient de limiter et de contrôler étroitement l'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application.	OUI							Un outil de gestion et de limitation du shadow IT est utilisé pour contôler l'utilisation de programmes et d'appplications non autorisés	Matrice des droits
9.4.5	Contrôle d'accès au code source des programmes	Il convient de restreindre l'accès au code source des programmes	OUI				X			Les scripts sont stockés dans des espaces sécurisés uniquement accessibles aux équipes de production	Liste des utilisateurs autorisés
10	**Cryptographie**										**SEPO12-Transfert et chifrement de l'information**
10.1	**Mesures cryptographiques**	**Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			
10.1.1	Politique d'utilisation des mesures cryptographiques	Il convient d'élaborer et de mettre en oeuvre une politique d'utilisation de mesures cryptographiques en vue de protéger l'information.	OUI	X	X	X	X			Politique édictée sur le chiffrement des flux et des données Cette politique est révisée réguliérement afin d'offrir le meilleur niveau de sécurité en adéquation avec les bonnes pratiques normalisées	Révision annuelle de cette politique
10.1.2	Gestion des clés	Il convient d'élaborer et de mettre en oeuvre tout au long de leur cycle de vie une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques	OUI			X	X			Administration des certificats pour accès HTTPS en accord avec les bonnes pratiques autorité de certifcation reconnue , stockage des clés dans un keyvault Gestion des clès de chiffrement de données stockées dans les Datacenter	Certificats administrés par Cegid et issus d'une CA reconnue Gestion des clés par Cegid (Cloud Privé) ou par le fournisseur (Cloud Publique)
11	**Sécurité physique et environnementale**										**SEPO1 Contôle des accès / SEPO6 Sécurité Physique et environnementale**
11.1	**Zones sécurisées**	**Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			
11.1.1	Périmètre de sécurité physique	Il convient de définir des périmètres de sécurité servant à protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information	OUI				X			Les équipes d'exploitation et de production sont dans des locaux isolés physiquement	Convention de service avec les services généraux
11.1.2	Contrôles physiques des accès	Il convient de protéger les zones sécurisées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis	OUI				X			Accès sécurisés et par badge aux locaux de Production aux seuls collaborateurs autorisés	Liste de contôle mensuel des accès
11.1.3	Sécurisation des bureaux, des salles et des équipements	Il convient de concevoir et d'appliquer des mesures de sécurité physique aux bureaux, aux salles et aux équipements	OUI				X			Portes vérouillées avec alarmes en cas d'ouverture prolongée	
11.1.4	Protection contre les menaces extérieures et environnementales	Il convient de concevoir et d'appliquer des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents	OUI		X	X	X	X		Protection du bâtiment hébergeant les équipes de production Alimentation,climatisation,câblage réseau ..	Contrat de service fournisseur interne avec les Services Généraux
11.1.5	Travail dans les zones sécurisées	Il convient de concevoir et d'appliquer des procédures pour le travail en zone sécurisée.	OUI							Protection du bâtiment hébergeant les équipes de production Alimentation,climatisation,câblage réseau .. Pour les locaux historiques de Talentsoft, il n'y a pas de travail en zones sécurisées. Cette exigence n'est donc pas incluse.	
11.1.6	Zones de livraison et de chargement	Il convient de contrôler les points d'accès tels que les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux et, si possible, de les isoler des moyens de traitement de l'information, de façon à éviter les accès non autorisés	OUI				X			Les livraisons sont effectuées au PC sécurité du bâtiment Le contôle est effectuée par une société de gardiennage privée sous le responsabilité des SG de Cegid Pour les locaux historiques de Talentsoft, il n'y a pas de zones de livraison. Cette exigence n'est donc pas incluse.	
11.2	**Matériels**	**Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**			

11.2.1	Emplacement et protection du matériel	Il convient de déterminer l'emplacement du matériel et de le protéger de manière à réduire les risques liés à des menaces et dangers environnementaux et les possibilités d'accès non autorisé.	OUI				X		Les matériels sensibles sont sockés dans des locaux sécurisés	Contrat de service fournisseur interne avec les Services Généraux
11.2.2	Services généraux	Il convient de protéger le matériel des coupures de courant et autres perturbations dues à une défaillance des services généraux.	OUI					X	Système d'alimentation électrique indépendant est opérationnel en cas de défaillance du système général	Contrat de mainteance fournisseur onduleur
11.2.3	Sécurité du câblage	Il convient de protéger les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information contre toute interception, interférence ou dommage.	OUI				X	X	Le réseau local de la production SaaS est un réseau switché physiquement indépendant du reste de l'entreprise	Configuration et shéma d'architecture réseau SaaS
11.2.4	Maintenance des matériels	Il convient d'entretenir le matériel correctement pour garantir sa disponibilité permanente et son intégrité	OUI				X	X	La maintenance des matériels internes et collaborateurs est sous traitée et contractualisée par la DSI	Contrat de service fournisseur interne avec la DSI
11.2.5	Sortie des actifs	Il convient de ne pas sortir un matériel, des informations ou des logiciels des locaux de l'organisation sans autorisation préalable	OUI						Formalisé dans la charte d'utilisation des outils et des moyens informatiques	
11.2.6	Sécurité du matériel et des actifs hors des locaux	Il convient d'appliquer des mesures de sécurité au matériel utilisé hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site.	OUI				X	X	Chiffrement des disques, Anti Virus, connexion à distance sécurisée par passerelle d'accès et/ou VPN	Contrat de service fournisseur interne avec la DSI
11.2.7	Mise au rebut ou recyclage sécurisé des matériels	Il convient de vérifier chacun des éléments du matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut ou sa réutilisation	OUI	X	X	X	X	X	Destruction des supports contenant des données clients ou en rapport avec ces données (poste des collaborateurs)	Preuves Destruction des Données par la production SaaS Contrat Cloud
11.2.8	Matériel utilisateur laissé sans surveillance	Il convient que les utilisateurs s'assurent que le matériel non surveillé est doté d'une protection appropriée	OUI				X	X	Cable antivol sur les postes collaborateurs	Vérouillage des écrans au bout de 15mn (stratégie AD)
11.2.9	Politique du bureau propre et de l'écran vérouillé	Il convient d'adopter une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide pour les moyens de traitement de l'information	OUI				X		Stockage des documents sur espace collaboratif privilégié Casier individuel de stockage - Broyeuse pour document à dipsosition Verouillage automatique des sessions en cas d'inactivité prolongée	
12	**Sécurité liée à l'exploitation**									**SEPO4 Sécurité liée à l'exploitation**
12.1	**Procédures et responsabilités liées à l'exploitation**	**S'assurer de l'exploitation correcte et sécurisée des moyens de traitement de l'information**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
12.1.1	Procédures d'exploitation documentées	Il convient de documenter les procédures d'exploitation et de les mettre à disposition de tous les utilisateurs concernés	OUI				X		Toutes les procédures d'explotation sont documentées et accessibles à tous les collaborateurs de SaaS dans la GED	Processus de Gestion des documents de la GED
12.1.2	Gestion des changements	Il convient de contrôler les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information qui influent sur la sécurité de l'information	OUI				X		Une instance hebdomadaire est planifiée sur la gestion des changements	CR et gestion des changes dans Inside
12.1.3	Dimensionnement	Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour garantir les performances exigées du système	OUI			X	X		Surveillance permanente de l'allocation des ressources Comité mensuel sur le dimensionnemnt des infrastructures et des ressources	Console de supervision Centreon Compte rendus de réunion de capacity planning Adaptation des RH à l'activité
12.1.4	Séparation des environnements de développement, de test et d'exploitation	Il convient de séparer les environnements de développement, de test et d'exploitation pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation	OUI			X	X		Segrégation assurée par le workflow automatisé dans AzureDevOps	Architecture Réseaux
12.2	**Protection contre les logiciels malveillants**	**Garantir que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
12.2.1	Mesures contre les logiciels malveillants	Il convient de mettre en oeuvre des mesures de détection, de prévention et de récupération, conjuguées une sensibilisation des utilisateurs adaptée, pour se protéger contre les logiciels malveillants	OUI				X	X	Antivirus / Antimalware centralisé et administré pour toutes les ressources	Console antivirale (MAJ du document à voir)
12.3	**Sauvegarde**	**Se protéger de la perte de données**	**Retenue**	**OL**	**OB**	**EB**	**BP**	**AR**		
12.3.1	Sauvegarde des informations	Il convient de réaliser des copies de sauvegarde de l'information, des logiciels et des images systèmes, et de les tester régulièrement conformément à une politique de sauvegarde convenue	OUI						La politique de sauvegarde prend en compte la spécificité de chaque offre client. Elle prend en compte la disponibilité, l'intégrite et la rétension.	Rapports de sauvegarde
12.4	**Journalisation et surveillance**	**Enregistrer les événements et générer des preuves.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
12.4.1	Journalisation des événements	Il convient de créer, de tenir à jour et de revoir régulièrement les journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information	OUI	X	X	X	X		Les événements relatifs à la sécurité de l'information sont centralisés dans un outil de concaténation des logs.Cet outil est régit par une politique bien définie	Consoles de centralisation des journaux (Splunk)
12.4.2	Protection de l'information journalisée	Il convient de protéger les moyens de journalisation et l'information journalisée contre les risques de falsification ou d'accès non autorisé	OUI	X			X		L'outil de gestion de logs est hébergé dans une architecture sécurisée (redondance,chiffrement des flux et des disques, gestion des accès, sauvegarde)	Consoles de centralisation des journaux (Splunk)
12.4.3	Journaux administrateur et opérateur	Il convient de journaliser les activités de l'administrateur système et de l'opérateur système, ainsi que de protéger et de revoir régulièrement les journaux.	OUI		X		X		Un rapport l automatique des journaux administrateurs et opérateurs est produit mensuellement	Rapport comptes administrateurs (Splunk)
12.4.4	Synchronisation des horloges	Il convient de synchroniser les horloges de l'ensemble des systèmes de traitement de l'information concernés d'une organisation ou d'un domaine de sécurité sur une source de référence temporelle unique	OUI		X		X	X	Une synchronisation NTP est configurée sur tous les actifs	Stratégies de groupes et doc NTP
12.5	**Maîtrise des logiciels en exploitation**	**Garantir l'intégrité des systèmes en exploitation**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
12.5.1	Installation de logiciels sur des systèmes en exploitation	Il convient de mettre en oeuvre des procédures pour contrôler l'installation de logiciels sur des systèmes en exploitation.	OUI				X	X	Un outil et une Console centralisée permette une gestion d'inventaire des logiciels en exploitation. Des Template d'installation sont utilisés pour la configurationdes serveurs virtuels	Consoles d'inventaire logiciel
12.6	**Gestion des vulnérabilités techniques**	**Empêcher toute exploitation des vulnérabilités techniques**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		**Sécurité Liée à l'Exploitation (SEPO4)**
12.6.1	Gestion des vulnérabilités techniques	Il convient d'être informé en temps voulu des vulnérabilités techniques des systèmes d'information en exploitation, d'évaluer l'exposition de l'organisation à ces vulnérabilités et de prendre les mesures appropriées pour traiter le risque associé	OUI				X	X	La gestion des vulnérabilité se fait par un outil de scan et par les alertes remontées par les C.E.R.T. Politiqe de traitement de ces vulnérabilités par périmétre en mode d'escalade	Compte Rendu des réunions de suivi sécurité des SI
12.6.2	Restrictions liées à l'installation de logiciels	Il convient d'établir et de mettre en oeuvre des règles régissant l'installation de logiciels par les utilisateurs	OUI				X		Politique de détection de shadowIT outillage sur les postes collaborateurs	Charte utilisation des outils
12.7	**Considérations sur l'audit des systèmes d'information**	**Réduire au minimum l'incidence des activités d'audit sur les systèmes en exploitation**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		**Sécurité Liée à l'Exploitation (SEPO4)**

12.7.1	Mesures relatives à l'audit des systèmes d'information	Pour réduire au minimum les perturbations subies par les processus métier, il convient de planifier avec soin et d'arrêter avec les personnes intéressées les exigences d'audit et les activités impliquant des contrôles des systèmes en exploitation	OUI				X	X	Les différentes politiques (Scan) et accords (Pentest) prennent en compte les périodes d'activités des métiers afin de minimiser les impacts	Modèles concernant les accords d'audit / Pentest
13	**Sécurité des communications**									**SEPO14-Management de la sécurité des réseaux**
13.1	**Gestion de la sécurité des réseaux**	**Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
13.1.1	Contrôle des réseaux	Il convient de gérer et de contrôler les réseaux pour protéger l'information contenue dans les systèmes et les applications	OUI				X	X	Les réseaux et les liens sont supervisés par les outils de surveillance. Les accès sont traçés et contrôlés	Procédure de ségrégation des droits et des équipes. Contrôle et logs des accès sur les équipements. Redondance des équipes des équipements et des ressources. Contrat de service Fournisseur Interne - DSI Un contrat de service portant sur la garantie de service est appliquée avec la DSI pour la partie LAN et la WAN Cloisonnement des réseaux par la mise en place de DMZ et de VLAN. Les réseaux et les liens sont supervisés en direct par les outils de surveillance.
13.1.2	Sécurité des services de réseau	Pour tous les services de réseau, il convient d'identifier les mécanismes de sécurité, les niveaux de service et les exigences de gestion, et de les intégrer dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés	OUI				X		Une convention de service interne est contractualisée annuellement avec la DSI Elle prend en compte la sécurité des réseaux	Les réseaux et les liens sont supervisés en direct par les outils de surveillance.
13.1.3	Cloisonnement des réseaux	Il convient que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient cloisonnés sur les réseaux	OUI				X		Cloisonnement des réseaux par la mise en place de DMZ et de VLAN.	Documents d'architecture réseau
13.2	**Transfert de l'information**	**Maintenir la sécurité de l'information transférée au sein de l'organisation et vers une entité extérieure.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		**SEPO2- Transfert et chiffrement de l'information**
13.2.1	Politiques et procédures de transfert de l'information	Il convient de mettre en place des politiques, des procédures et des mesures de transfert formelles pour protéger les transferts d'information transitant par tous types d'équipements de communication	OUI				X		Une politique énonçant les régles de chiffrements et de sécurité des communications est établie. Elle est révisée périodiquement.	
13.2.2	Accords en matière de transfert d'information	Il convient que les accords traitent du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers	OUI			X	X		Les protocoles sécurisés d'échanges utilisés avec les tiers permetteent de garantir l'intégrité , la confidentialité et la non répudiation des informations	
13.2.3	Messagerie électronique	Il convient de protéger de manière appropriée l'information transitant par la messagerie électronique	OUI				X	X	La messagerie électronique n'utilise que des processus sécurisé (flux , authentification)	Configuration serveur de messagerie
13.2.4	Engagements de confidentialité ou de non-divulgation	Il convient d'identifier, de revoir régulièrement et de documenter les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisation en matière de protection de l'information	OUI		X		X		L'ensemble du personnel Cegid intervenant sur des données confidentielles signe un engagement de confidentialité sans limite de temps, impliquant des mesures disciplinaires ou poursuites en cas de non-respect.	Processus RH
14	**Acquisition, développement et maintenance des systèmes d'information**									**SEPO8-Politique de sécurité de l'information dans la gestion de projet**
14.1	**Exigences de sécurité applicables aux systèmes d'information**	**Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut notamment des exigences spécifiques pour les systèmes d'information fournissant des services sur les réseaux publics.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		**SEPO2- Transfert et chiffrement de l'information**
14.1.1	Analyse et spécification des exigences de sécurité de l'information	Il convient que les exigences liées à la sécurité de l'information figurent dans les exigences des nouveaux systèmes d'information ou des changements apportés aux systèmes existants	OUI				X	X	Des procédures formalisée sur la sécurité sont intégrées dans tous les projets et tout au long du cycle de vie du projet	Questionnaires d'expression des besoins sécurité du projet
14.1.2	Sécurisation des services d'application sur les réseaux publics	Il convient de protéger l'information liée aux services d'application transmise sur les réseaux publics contre les activités frauduleuses, les différends contractuels, ainsi que la divulgation et la modification non autorisées.	OUI	X			X	X	Protection périmétrique des accès au réseaux publics (Pare Feu , Sonde IDS/IPS) Chiffrement des flux par certificats issus d'une autotité de certification reconnue, les clés sont stockées dans un coffre fort numérique	Politique de transfert et chiffrement de l'information
14.1.3	Protection des transactions liées aux services d'application	Il convient de protéger l'information impliquée dans les transactions liées aux services d'application pour empêcher une transmission incomplète, des erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou sa réémission.	OUI				X	X	Utilisation de protocoles sécurisés garantissant une transmission complète sans modification,possible de l'information et interdisant, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée .	
14.2	**Sécurité des processus de développement et d'assistance technique**	**S'assurer que les questions de sécurité de l'information sont étudiées et mises en oeuvre dans le cadre du cycle de développement des systèmes d'information**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		**SEPO15 - Politique de développement sécurisé**
14.2.1	Politique de développement sécurisé	Il convient d'établir des règles de développement des logiciels et des systèmes, et de les appliquer aux développements de l'organisation	OUI				X		Une politique décrit et cadre la sécurité des processus de développement	STRATUS
14.2.2	Procédures de contrôle des changements de système	Il convient de contrôler les changements apportés au système dans le cycle de développement en utilisant des procédures formelles de contrôle des changements	OUI				X		Les changments standards sont opérés via le worflow de l'orchestrateur de la plateforme. Les changements non standard sont traités par le processus de change	
14.2.3	Revue technique des applications après changement apporté à la plateformed'exploitation	Lorsque des changements sont apportés aux plateformes d'exploitation, il convient de revoir et de tester les applications critiques métier afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité	OUI				X	X	Les mises à jour matériel et/ou systéme sont testés sur des groupes pilotes avant application sur les environnements de production	Processus de mises à jour des systèmes
14.2.4	Restrictions relatives aux changements apportés aux progiciels	Il convient de ne pas encourager la modification des progiciels et de se limiter aux changements nécessaires. Il convient également d'exercer un contrôle strict sur ces changements	OUI				X		Tous les changements relatifs aux scrips et automates sont consignés dans un git	Pas de modification du code des progiciels utilisés
14.2.5	Principes d'ingénierie de la sécurité des systèmes	Il convient d'établir, de documenter, de tenir à jour et d'appliquer des principes d'ingénierie de la sécurité des systèmes à tous les travaux de mise en oeuvre de systèmes d'information.					X		Les scripts et automates sont normalisés et testés avant mise en production	Formation/Sensibilisation
14.2.6	Environnement de développement sécurisé	Il convient que les organisations établissent un environnement de développement sécurisé pour les tâches de développement et d'intégration du système, qui englobe l'intégralité du cycle de développement du système, et qu'ils en assurent la protection de manière appropriée	OUI				X		Gérer par le workflow AzureDevOps et les serveurs de développement	Architecture Réseaux
14.2.7	Développement externalisé	Il convient que l'organisation supervise et contrôle l'activité de développement du système externalisé	OUI		X		X		Une convention de service interne avec les BU de développement supervise et contôle les activités et applications externes au SMSI	
14.2.8	Test de la sécurité du système	Il convient de réaliser les tests de fonctionnalité de la sécurité pendant le développement	OUI				X		Les phases de test et les tests de conformité sont assurés dans	

14.2.9	Test de conformité du système	Il convient de déterminer des programmes de test de conformité et des critères associés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions	OUI				X		Les phases de test et les tests de conformité sont assurés dans le workflow AzureDevOps	Résultat Scan vulnérabilité (I/O Tenable)
14.3	**Données de test**	**Garantir la protection des données utilisées pour les tests**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
14.3.1	Protection des données de test	Il convient que les données de test soient sélectionnées avec soin, protégées et contrôlées	OUI				X		Gérer par le workflow AzureDevOps et les serveurs de développement	Journalisation de la copie
15	**Relations avec les fournisseurs**									**SEP013-Relaion avec les fournisseurs**
15.1	**Sécurité dans les relations avec les fournisseurs**	**Garantir la protection des actifs de l'organisation accessibles aux fournisseurs**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
15.1.1	Politique de sécurité de l'information dans les relations avec les fournisseurs	Il convient de convenir avec le fournisseur les exigences de sécurité de l'information pour limiter les risques résultant de l'accès du fournisseur aux actifs de l'organisation et de les documenter.	OUI	X	X	X	X	X	La poltique de sécurité dans les relations fournisseurs prend en compte et décrit les besoins et mesures de sécurité nécessaires pour respecter les obligations légales, réglementaires et contractuelles de Cegid	
15.1.2	La sécurité dans les accords conclus avec les fournisseurs	Il convient que les exigences applicables liées à la sécurité de l'information soient établies et convenues avec chaque fournisseur pouvant avoir accès, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation	OUI	X	X		X	X	Cegid s'assure de l'implication de ses fournisseurs dans la sécurité du service délivré au travers de certification et d'engagement contractuel	
15.1.3	Chaine d'approvisionnement des produits et des services informatique	Il convient que les accords conclus avec les fournisseurs incluent des exigences sur le traitement des risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et des services informatiques	OUI	X	X		X	X	Cegid s'assure de l'implication de ses fournisseurs dans la sécurité du service délivré au travers de certification et d'engagement contractuel Pour les activités historiques de Talentsoft, il n'y a pas d'approvisionnement dans le cadre de la production, celle-ci est sous la responsabilité de Quadria. Cette exigence n'est donc pas incluse.	
15.2	**Gestion de la prestation du service**	**Maintenir un niveau convenu de sécurité de l'information et de prestation de services, conformément aux accords conclus avec les fournisseurs**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
15.2.1	Surveillance et revue des services des fournisseurs	Il convient que les organisations surveillent, revoient et auditent à intervalles réguliers la prestation des services assurés par les fournisseurs	OUI	X	X		X		Des comités de pilotage de la sécurité sont planifiés et organisés de façon récurrente avec les fournisseurs. Des audits permettent l'évaluation de l'évolution et des changements dans le cadre contractuel	CR Comité de sécurité Kyndryl/Microsoft
15.2.2	Gestion des changements apportés dans les services des fournisseurs	Il convient de gérer les changements effectués dans les prestations de service des fournisseurs, y compris le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation du risque	OUI	X	X		X			
16	**Gestion des incidents liés à la sécurité de l'information**									**SEPS3-Gestion des incidents de sécurité**
16.1	**Gestion des incidents liés à la sécurité de l'information et améliorations**	**Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
16.1.1	Responsabilités et procédures	Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information	OUI	X		X	X	X		
16.1.2	Signalement des événements liés à la sécurité de l'information	Il convient de signaler, dans les meilleurs délais, les événements liés à la sécurité de l'information, par les voies hiérarchiques appropriées	OUI	X		X	X	X		
16.1.3	Signalement des failles liées à la sécurité de l'information	Il convient d'enjoindre tous les salariés et contractants utilisant les systèmes et services d'information de l'organisation à noter et à signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services	OUI	X		X	X	X	Processus de gestion des incidents de sécurité en conformaité avec ISO 27035 comprenant Signalement de l'événement de sécurité Préqualification de l'événement Phase de qualification Investigation Communication / Déclaration Traitement Retour d'expérience Clôture de l'incident Une matrice de type RACI détermine les rôles et responsabilité pour chaque phase Une revue hebdomadaire des incidents est effectuée	
16.1.4	Appréciation des événements liés à la sécurité de l'information et prise de décision	Il convient d'apprécier les événements liés à la sécurité de l'information et de décider s'ils doivent être classés comme incidents liés à la sécurité de l'information	OUI	X		X	X	X		Stratus
16.1.5	Réponse aux incidents liés à la sécurité de l'information	Il convient de répondre aux incidents liés à la sécurité de l'information conformément aux procédures documentées.	OUI	X		X	X	X		
16.1.6	Tirer des enseignements des incidents liés à la sécurité de l'information	Il convient de tirer parti des connaissances recueillies suite à l'analyse et la résolution des incidents liés à la sécurité de l'information pour réduire la probabilité ou les conséquences d'incidents ultérieurs	OUI	X		X	X	X		
16.1.7	Collecte de preuves	Il convient que l'organisation définisse et applique des procédures d'identification, de recueil, d'acquisition et de protection de l'information pouvant servir de preuve	OUI	X		X	X	X		
17	**Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité**									**SEIT25-Gestion de crise SaaS**
17.1	**Continuité de la sécurité de l'information**	**Il convient que la continuité de la sécurité de l'information fasse partie intégrante des systèmes de gestion de la continuité de l'activité**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
17.1.1	Organisation de la continuité de la sécurité de l'information	Il convient que l'organisation détermine ses exigences en matière de sécurité de l'information et de continuité du management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre	OUI			X	X		Une politique de continuité des affaires encadre l'organisation et les processus de continuité de la sécurité de l'information Un processus "code rouge" réglemente la gestion de crise	
17.1.2	Mise en oeuvre de la continuité de la sécurité de l'information	Il convient que l'organisation établisse, documente, mette en oeuvre et maintienne à jour des processus, des procédures et des mesures permettant de garantir le niveau requis de continuité de la sécurité de l'information au cours d'une situation défavorable	OUI			X	X		Différents processus permettent la continuité de la sécurité de l'information (Sauvegarde des données , résilience des infrastructures et des ressources humaines , administration des outils de production sécurisée à distance)	Gestion des incidents / Code Rouge
17.1.3	Vérifier, revoir et évaluer la continuité de la sécurité de l'information	Il convient que l'organisation vérifie à intervalles réguliers les mesures de continuité de la sécurité de l'information déterminées et mises en oeuvre, afin que s'assurer qu'elles restent valables et efficaces dans des situations défavorables	OUI			X	X		La continuité de la sécurité des informations est évaluée de façon récurrente	
17.2	**Redondances**	**Garantir la disponibilité des moyens de traitement de l'information**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		

17.2.1	Disponibilité des moyens de traitement de l'information	Il convient de mettre en oeuvre des moyens de traitement de l'information avec suffisamment de redondances pour répondre aux exigences de disponibilité	OUI		X	X	X		Des mécanismes de redondance et de résilience des architectures et des équipes sont actifs de bout en bout. Il y a une supervision constante de ces mécanismes	Documents d'architectures SaaS
18	**Conformité**									**SEPO10-Gestion de la conformaité et des audits**
18.1	**Conformité aux obligations légales et réglementaires**	**Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
18.1.1	Identification de la législation et des exigences contractuelles applicables	Il convient, pour chaque système d'information et pour l'organisation elle-même, de définir, documenter et mettre à jour explicitement toutes les exigences légales, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences	OUI		X	X		X	Le processus juridique du groupe Cegid définis, documente et met à jours toutes les exigences légales, réglementaires et contractuelles applicables au SMSI	Processus Juridique
18.1.2	Droits de propriété intellectuelle	Il convient de mettre en oeuvre des procédures appropriées visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives aux droits de propriété intellectuelle et à l'utilisation de logiciels propriétaires	OUI		X	X		X	Cegid Cloud Factory s'engage à garantir la conformité avec les exigences légales, réglementaire et contractuelles relatives aux droits de la propriété intellectuelle et à l'utilisation des logiciels propriétaires. Les logiciels sont acquis à partir de sources connues et réputées afin de s'assurer du respect des droits d'auteur.	Registre des licences
18.1.3	Protection des enregistrements	Il convient de protéger les enregistrements de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier	OUI		X	X		X	Les enregistrements sont protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisés.	
18.1.4	Protection de la vie privée et protection des données à caractère personnel	Il convient de garantir la protection de la vie privée et la protection des données à caractère personnel telles que l'exigent la législation et les réglementations applicables, le cas échéant	OUI		X	X		X	Le règlement général sur la protection des données personnelles est applicable sur le périmètre depuis le 25 mai 2018. Dans ce cadre, Cegid a nommé un DPO qui est en charge de suivre le sujet de manière transverse au niveau du groupe	
18.1.5	Réglementation relative aux mesures cryptographiques	Il convient de prendre des mesures cryptographiques conformément aux accords, lois et réglementations applicables	OUI						Cegid Cloud Factory respecte les accords, lois et réglementations applicables relatives à la cryptographies. Cegid n'importe pas ou n'exporte pas de solution de cryptographie.	
18.2	**Revue de la sécurité de l'information**	**Garantir que la sécurité de l'information est mise en oeuvre et appliquée conformément aux politiques et procédures organisationnelles**	**Retenue**	**OL**	**OC**	**EB**	**BP**	**AR**		
18.2.1	Revue indépendante de la sécurité de l'information	Il convient de procéder à des revues régulières et indépendantes de l'approche retenue par l'organisation pour gérer et mettre en oeuvre la sécurité de l'information (à savoir le suivi des objectifs, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) à intervalles définis ou lorsque des changements importants sont intervenus	OUI					X	Cegid Cloud Factory réalise au moins une fois par an un audit interne du système d'information. Une revue de Direction est planifiée à l'issus	
18.2.2	Conformité avec les politiques et les normes de sécurité	Il convient que les responsables revoient régulièrement la conformité du traitement de l'information et des procédures dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité								Indicateurs et Objectifs SMSI
18.2.3	Vérification de la conformité technique	Il convient que les systèmes d'information soient régulièrement revus pour vérifier leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation	OUI			X	X		Une politique de pentests et d'audit technique permet d'identifier les écatrs	Rapport de Scan