cegid

Déclaration d'applicabilité

ISO27001:2022

Certificat N° : 666376 **Version du 05/03/2026** **Modifiée par : Equipe sécurité**
Classification : Public

ISO27001:2022

		Solution mise en œuvre
4	**Contexte de l'organisation**	
4.1	Compréhension de l'organisation et son contexte	
4.2	Compréhension des besoins et des attentes des parties intéressées	
4.3	Détermination du domaine d'application du système de management de la sécurité de l'information	Périmètre du Système de Management de la sécurité du SaaS
4.4	Système de management de la sécurité de l'information	
5	**Leadership**	
5.1	Leadership et engagement	
5.2	Politique	Gestion de la Gouvernance, des rôles et des responsabilités SMSI
5.3	Rôles, responsabilités et autorités au sein de l'organisation	
6	**Planification**	
6.1	Actions liées aux risques et opportunités	
6.2	Objectifs de sécurité de l'information et plans pour les atteindre	Processus d'Évaluation et de Traitement du Risque
6.3	Planification des modifications	
7	**Support**	
7.1	Ressources	
7.2	Compétence	Sécurité des Ressources Humaines
7.3	Sensibilisation	
7.4	Communication	Processus Communication du SMSI
7.5	Informations Documentées	Processus de gestion de la documentation
8	**Fonctionnement**	
8.1	Planification et contrôle opérationnels	Politique de contrôle, surveillance et Amélioration
8.2	Appreciation des risques de sécurité de l'information	Processus de gestion des risques
8.3	Traitement des risques de sécurité de l'information	
9	**Evaluation des performances**	
9.1	Surveillance, mesures, analyse et évaluation	Politique de contrôle, surveillance et Amélioration
9.2	Audit interne	Gestion de la conformité et des audits
9.3	Revue de direction	Gestion de la Gouvernance, des rôles et des responsabilités SMSI
10	**Amélioration**	
10.1	Amélioration continue	Politique de contrôle, surveillance et amélioration
10.2	Non-conformité et action corrective	Gestion de la conformité et des audits

La mise en œuvre des contrôles de sécurité définis dans la déclaration d'applicabilité visent à réduire les risques de sécurité pouvant exister dans le SMSI.

ISO 27001 - Annexe A1

ISO27001:2022	Processus / Capacités opérationnelles	Exigences		Applicable (Inclusion)	Justification d'inclusion de la mesure	Mise en œuvre de la mesure	Solution mise en œuvre
				2 valeurs _ OUI _ NON		2 valeurs _ OUI _ NON	
Mesures de sécurité organisationnelles							
5.1	#Gouvernance	Politiques de sécurité de l'information	Il convient de définir une politique de sécurité de l'information et des politiques spécifiques à une thématique, de les faire approuver par la direction, de les publier, de les communiquer et d'en demander confirmation au personnel et aux parties intéressées concernés, ainsi que de les réviser à intervalles planifiés et si des changements significatifs ont lieu.	OUI	Analyse de risques	OUI	Une politique de sécurité de l'information a été rédigée Elle est révisée annuellement et approuvée par la Direction des services Cloud
5.2	#Gouvernance	Fonctions et responsabilités liées à la sécurité de l'information	Il convient de définir et d'attribuer les fonctions et responsabilités liées à la sécurité de l'information selon les besoins de l'organisation.	OUI	Analyse de risques	OUI	L'équipe sécurité groupe est organisée de manière transverse. Elle est indépendante hiérarchiquement et opérationnellement des activités du SMSI
5.3	#Gouvernance	Séparation des tâches	Il convient de séparer les tâches et domaines de responsabilité incompatibles.	OUI	Analyse de risques	OUI	Organisation de type DevOps des missions et des équipes
5.4	#Gouvernance	Responsabilités de la direction	Il convient que la direction demande à tout le personnel d'appliquer les mesures de sécurité del'information conformément à la politique de securité de l'information, aux politiques spécifiques à une thématique et aux procédures établies de l'organisation.	OUI	Analyse de risques	OUI	Engagement formel de la Direction des services Cloud au travers des différents comités , réunions et communications autour de la sécurité et du SMSI
5.5	#Gouvernance	Contacts avec les autorités	Il convient que l'organisation établisse et maintienne le contact avec les autorités appropriées.	OUI	Analyse de risques	OUI	L'équipe Sécurité de Cegid entretient des échanges réguliers avec la CNIL et l'ANSSI
5.6	#Gouvernance	Contact avec des groupes de d'interet spécifiques	Il convient que l'organisation établisse et maintienne des contacts avec des groupes d'intérêt spécifiques ou autres forums spécialisés sur la sécurité et associations professionnelles.	OUI	Analyse de risques	OUI	Les collaborateurs de l'équipe Sécurité de Cegid sont membres des associations suivantes: CLUSIF, Club ISO27001, Club de la continuité d'Activité, Incibe,...
5.7	#Gestion_des_menaces_et_des_vulnérabilités	Renseignements sur les menaces	Il convient de collecter et d'analyser les informations relatives aux menaces de sécurité de l'information pour produire les renseignements sur les menaces.	OUI	Analyse de risques	OUI	Abonnement à un service de veille mondiale. Réunions biannuelles des SMSI Managers pour analyse, Politique treath inteligence
5.8	#Gouvernance	Sécurité de l'information dans la gestion de projet	Il convient d'intégrer la sécurité de l'information dans la gestion de projet.	OUI	Analyse de risques	OUI	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
5.9	#Gestion_des_actifs	Inventaire des informations et autres actifs associés	Il convient d'élaborer et de tenir à jour un inventaire des informations et autres actifs associés, y compris leurs propriétaires.	OUI	Analyse de risques	OUI	L'inventaire des actifs est revu et mis à jour dans l'outil d'analyse de risques. Les actifs sont la propriété de la Direction des services Cloud
5.10	#Gestion_des_actifs #Protection_des_informations	Utilisation correcte des informations et autres actifs associés	Il convient d'identifier, de documenter et de mettre en oeuvre les règles d'utilisation correcte et les procédures de traitement des informations et autres actifs associés.	OUI	Analyse de risques	OUI	Une charte d'utilisation des outils informatiques à destination des collaborateurs est communiquée
5.11	#Gestion_des_actifs	Restitution des actifs	Il convient que le personnel et les autres parties intéressées, selon le cas, restituent tous les actifs de l'organisation qui sont en leur possession au moment du changement ou de la fin de leur emploi, contrat ou accord.	OUI	Analyse de risques	OUI	Restitution des actifs suivant l'inventaire de la fiche de départ collaborateur sous la responsabilité du manager
5.12	#Protection_des_informations	Classification des information	Il convient de classifier les informations conformément aux besoins de sécurité de l'information de l'organisation, sur la base des exigences de confidentialité, d'intégrité, de disponibilité et des exigences importantes des parties intéressées.	OUI	Analyse de risques	OUI	Les informations sont classifiées
5.13	#Protection_des_informations	Marquage des informations	Il convient d'élaborer et de mettre en oeuvre un ensemble approprié de procédures pour le marquage des informations, conformément au schéma de classification des informations adopté par l'organisation.	OUI	Analyse de risques	OUI	L'ensemble des actifs (documentaires , actifs clients) est soumis à la politique de gestion des actifs. Cette politique prend en compte le niveau de classification des actifs associé à son niveau de diffusion et de chiffrement nécessaire à sa diffusion
5.14	#Gestion_des_actifs #Protection_des_informations	Transfert des informations	Il convient de mettre en place des règles, procédures ou accords sur le transfert des informations pour tous les types de moyens de transfert au sein de l'organisation, et entre l'organisation et des tierces parties.	OUI	Analyse de risques	OUI	Une politique énonçant les règles de chiffrements et de sécurité des communications est établie. Elle est révisée périodiquement. Les protocoles sécurisés d'échanges utilisés avec les tiers permettent de garantir l'intégrité , la confidentialité et la non répudiation des informations. Utilisation des protocoles sécurisés par la messagerie électronique
5.15	#Gestion_des_identités_et_des_accès	Contrôle d'accès	Il convient de définir et de mettre en oeuvre des règles visant à contrôler l'accès physique et logique aux informations et autres actifs associés en fonction des exigences métier et de sécurité de l'information.	OUI	Analyse de risques	OUI	Politique de contrôle des accès

5.16	#Gestion_des_identités_et_des_accès	Gestion des identités	Il convient de gérer le cycle de vie complet des identités.	OUI	Analyse de risques	OUI	Gestion des inscriptions/désinscriptions des utilisateurs dans notre outil d'orchestration de la plateforme Cegid Cloud
5.17	#Gestion_des_identités_et_des_accès	Informations d'authentifications	Il convient que l'attribution et la gestion des informations d'authentification soient contrôlées par un processus de gestion, incluant des recommandations au personnel sur l'utilisation appropriée des informations d'authentification.	OUI	Analyse de risques	OUI	Des règles d'utilisation des informations secrètes sont clairement définis dans la charte d'utilisation des outils informatique
5.18	#Gestion_des_identités_et_des_accès	Contrôle d'accès	Il convient que les droits d'accès aux informations et autres actifs associés soient pourvus, révisés, modifiés et supprimés conformément à la politique spécifique à la thématique du contrôle d'accès et aux règles de contrôle d'accès de l'organisation.	OUI	Analyse de risques	OUI	Gestion des inscriptions/désinscriptions des utilisateurs dans notre outil d'orchestration de la plateforme Cegid Cloud
5.19	#Sécurité_des_relations_fournisseurs	Sécurité de l'information dans les relations avec les fournisseurs	Il convient d'établir et de convenir des exigences de sécurité de l'information appropriées avec chaque fournisseur, selon le type de relation avec le fournisseur.	OUI	Analyse de risques	OUI	La politique 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
5.20	#Sécurité_des_relations_fournisseurs	Prise en compte de la sécurité de l'information dans les accords conclus avec les fournisseurs	Il convient d'établir et de convenir des exigences de sécurité de l'information appropriées avec chaque fournisseur, selon le type de relation avec le fournisseur.	OUI	Analyse de risques	OUI	Cegid s'assure de l'implication de ses fournisseurs dans la sécurité du service délivré au travers de certification et d'engagement contractuel
5.21	#Sécurité_des_relations_fournisseurs	Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC	Il convient de définir et de mettre en oeuvre des processus et procédures pour gérer les risques de sécurité de l'information associés à la chaîne d'approvisionnement des produits et services TIC.	OUI	Analyse de risques	OUI	Cegid s'assure de l'implication de ses fournisseurs dans la sécurité du service délivré au travers de certification et d'engagement contractuel
5.22	#Sécurité_des_relations_fournisseurs #Assurance_de_sécurité_de_l'information	Surveillance, révision et gestion des changements des services fournisseurs	Il convient que l'organisation procède régulièrement à la surveillance, à la révision, à l'évaluation et à la gestion des changements des pratiques de sécurité de l'information du fournisseur et de prestation de services.	OUI	Analyse de risques	OUI	Des comités de pilotage de la sécurité sont planifiés et organisés de façon récurrente avec les principaux fournisseurs. Cegid Cloud surveille les certification de sécurité de l'information de ses fournisseurs
5.23	#Sécurité_des_relations_fournisseurs	Sécurité de l'information dans l'utilisation de services en nuage	Il convient que les processus d'acquisition, d'utilisation, de gestion et de cessation des services en nuage soient établis conformément aux exigences de sécurité de l'information de l'organisation.	OUI	Analyse de risques	OUI	Cegid s'assure que les contrats avec les fournisseurs de services en nuage sont conformes aux exigences de sécurité de l'information de l'organisation.
5.24	#Gouvernance, #Gestion_des_événements_de_sécurité_de_l'information	Planification et préparation de la gestion des incidents de sécurité de l'information	Il convient que l'organisation planifie et prépare la gestion des incidents de sécurité de l'information en procédant à la définition, à l'établissement et à la communication des processus, fonctions et responsabilités liés à la gestion des incidents de sécurité de l'information.	OUI	Analyse de risques	OUI	Processus de gestion des incidents de sécurité (voir Plan d'assurance Sécurité pour plus de détails)
5.25	#Gestion_des_événements_de_sécurité_de_l'information	Appréciation des événements de sécurité de l'information et prise de décision	Il convient que l'organisation évalue les événements de sécurité de l'information et décide s'ils doivent être catégorisés comme des incidents de sécurité de l'information.	OUI	Analyse de risques	OUI	
5.26	#Gestion_des_événements_de_sécurité_de_l'information	Réponse aux incidents de sécurité de l'information	Il convient de répondre aux incidents de sécurité de l'information conformément aux procédures documentées.	OUI	Analyse de risques	OUI	
5.27	#Gestion_des_événements_de_sécurité_de_l'information	Tirer des enseignements des incidents de sécurité de l'information	Il convient que les connaissances acquises à partir des incidents de sécurité de l'information soient utilisées pour renforcer et améliorer les mesures de sécurité de l'information.	OUI	Analyse de risques	OUI	
5.28	#Gestion_des_événements_de_sécurité_de_l'information	Recueil de preuves	Il convient que l'organisation établisse et mette en oeuvre des procédures pour l'identification, la collecte, l'acquisition et la préservation des preuves relatives aux événements de sécurité de l'information.	OUI	Analyse de risques	OUI	
5.29	#Continuité	Sécurité de l'information durant une perturbation	Il convient que l'organisation planifie comment maintenir la sécurité de l'information au niveau approprié pendant une perturbation.	OUI	Analyse de risques	OUI	Une politique de continuité des affaires encadre l'organisation et les processus de continuité de la sécurtité de l'information
5.30	#Continuité	Préparation des TIC pour la continuité d'activité	Il convient que la préparation des TIC soit planifiée, mise en oeuvre, maintenue et testée en se basant sur les objectifs de continuité d'activité et des exigences de continuité des TIC.	OUI	Analyse de risques	OUI	
5.31	#Réglementation_et_conformité	Exigences légales, statutaires, réglementaires et contractuelles	Il convient que les exigences légales, statutaires, réglementaires et contractuelles pertinentes pour la sécurité de l'information, ainsi que l'approche de l'organisation pour respecter ces exigences, soient identifiées, documentées et tenues à jour.	OUI	Analyse de risques	OUI	Le processus juridique du groupe Cegid définis, documente et met à jours toutes les exigences légales, réglementaires et contractuelles applicables au SMSI. Cegid Cloud respecte les accords, lois et réglementations applicables relatives à la cryptographies. Cegid n'importe pas ou n'exporte pas de solution de cryptographie.
5.32	#Réglementation_et_conformité	Droits de propriété intellectuelle	Il convient que l'organisation mette en oeuvre les procédures appropriées pour protéger les droits de propriété intellectuelle.	OUI	Analyse de risques	OUI	Cegid Cloud 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.
5.33	#Réglementation_et_conformité #Gestion_des_actifs #Protection_des_informations	Protection des enregistrements	Il convient que les enregistrements soient protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées.	OUI	Analyse de risques	OUI	Les enregistrements sont protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisés.
5.34	#Protection_des_informations #Réglementation_et_conformité	Protection de la vie privée et des DCP	Il convient que l'organisation identifie et respecte les exigences relatives à la protection de la vie privée et des DCP conformément aux lois, réglementations et exigences contractuelles applicables.	OUI	Analyse de risques	OUI	Le réglement 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
5.35	#Assurance_de_sécurité_de_l'information	Révision indépendante de la sécurité de l'information	Il convient que l'approche de l'organisation pour gérer la sécurité de l'information et sa mise en oeuvre, y compris les personnes, les processus et les technologies, soit revisée de manière indépendante à intervalles planifiés, ou lorsque des changements significatifs se produisent.	OUI	Analyse de risques	OUI	Cegid Cloud réalise au moins une fois par an un audit interne du système d'information. Une revue de Direction est planifiée à l'issus
5.36	#Réglementation_et_conformité #Assurance_de_sécurité_de_l'information	Conformité aux politiques, règles et normes de sécurité de l'information	Il convient que la conformité à la politique de sécurité de l'information, aux politiques spécifiques à une thématique, aux règles et aux normes de l'organisation soit régulièrement vérifiée.	OUI	Analyse de risques	OUI	
5.37	#Gestion_des_actifs #Sécurité_physique #Sécurité_système_et_réseau #Sécurité_des_applications #Configuration_sécurisée #Gestion_des_identités_et_des_accès #Gestion_des_menaces_et_des_vulnérabilités #Continuité #Gestion_des_événements_de_sécurité_de_l'information	Procédures d'exploitation documentées	Il convient que les procédures d'exploitation des moyens de traitement de l'information soient documentées et mises à disposition du personnel qui en a besoin.	OUI	Analyse de risques	OUI	Toutes les procédures d'explotation sont documentées et accessibles à tous les collaborateurs de SaaS dans la GED
Mesures de sécurité applicables aux personnes							
6.1	#Sécurité_des_ressources_humaines	Sélection des candidats	Il convient que des vérifications des références de tous les candidats à l'embauche soient réalisées avant qu'ils n'intègrent l'organisation puis de façon continue en tenant compte des lois, des réglementations et de l'éthique applicables, et il convient qu'elles soient proportionnelles aux exigences métier, à la classification des informations auxquelles ils auront accès et aux risques identifiés.	OUI	Analyse de risques	OUI	Des contrôles (Informations sur le CV, les Diplômes, extrait de casier judiciaire ...) sont effectués lors du recrutement et de l'intégration des candidats.
6.2	#Sécurité_des_ressources_humaines	Termes et conditions du contrat de travail	Il convient que les contrats de travail indiquent les responsabilités du personnel et de l'organisation en matière de sécurité de l'information.	OUI	Analyse de risques	OUI	Le contrat de travail signé par les nouveaux salariés comporte une clause de confidentialité et une clause de non concurrence
6.3	#Sécurité_des_ressources_humaines	Sensibilisation, enseignement et formation en sécurité de l'information	Il convient que le personnel de l'organisation et les parties intéressées pertinentes reçoivent une sensibilisation, un enseignement et des formations en sécurité de l'information appropriés, ainsi que des mises à jour régulières de la politique de sécurité de l'information, des politiques spécifiques à une thématique et des procédures de l'organisation qui soient pertinentes pour leur fonction.	OUI	Analyse de risques	OUI	Une formation sécurité nouveaux collaborateurs est systématiquement dispensée Un plan annuel de sensibilisation est élaboré et suivi
6.4	#Sécurité_des_ressources_humaines	Processus disciplinaire	Il convient de formaliser et de communiquer un processus disciplinaire permettant de prendre des mesures à l'encontre du personnel et d'autres parties intéressées qui ont commis une violation de la politique de securité de l'information.	OUI	Analyse de risques	OUI	Un processus disciplinaire peut être engagé en cas de manquement à la charte d'utilisation des outils et des matériels informatiques
6.5	#Sécurité_des_ressources_humaines #Gestion_des_actifs	Responsabilités après la fin ou le changement d'un emploi	Il convient que les responsabilités et les obligations relatives à la sécurité de l'information qui restent valables après la fin ou le changement d'un emploi, soient définies, appliquées et communiquées au personnel et autres parties intéressées pertinents.	OUI	Analyse de risques	OUI	Le collaborateur est informé de ses responsabilités en cas de modification de rupture ou de fin de contrat par son correspondant RH
6.6	#Human_resource_security #Information_protection	Accords de confidentialité ou de non-divulgation	Il convient que les responsabilités et les obligations relatives à la sécurité de l'information qui restent valables après la fin ou le changement d'un emploi, soient définies, appliquées et communiquées au personnel et autres parties intéressées pertinents.	OUI	Analyse de risques	OUI	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.
6.7	#Gestion_des_actifs #Protection_des_informations #Sécurité_physique #Sécurité_système_et_réseau	Travail à distance	Il convient de mettre en oeuvre des mesures de sécurité lorsque le personnel travaille à distance, pour protéger les informations accessibles, traitées ou stockées en dehors des locaux de l'organisation.	OUI	Analyse de risques	OUI	Chiffrement des disques des laptops des collaborateurs Filtres de confidentialité MFA et VPN en situation de mobilité

6.8	#Gestion_des_événements_de_sécurité_de_l'information	Déclaration des événements de sécurité de l'information	Il convient que l'organisation fournisse un mécanisme au personnel pour déclarer rapidement les événements de sécurité de l'information observés ou suspectés, à travers des canaux appropriés.	OUI	Analyse de risques	OUI	Processus de gestion des incidents de sécurité (voir Plan d'assurance Sécurité pour plus de détails)
Mesures de sécurité physique							
7.1	#Sécurité_physique	Périmètres de sécurité physique	Il convient que les périmètres de sécurité soient définis et utilisés pour protéger les zones qui contiennent les informations et autres actifs associés.	OUI	Analyse de risques	OUI	Les équipes d'exploitation et de production sont dans des locaux isolés physiquement
7.2	#Sécurité_physique #Gestion_des_identités_et_des_accès	Les entrées physiques	Il convient de protéger les zones sécurisées par des mesures de sécurité des accès et des points d'accès appropriées.	OUI	Analyse de risques	OUI	Accès sécurisés et par badge aux locaux de Production aux seuls collaborateurs autorisés
7.3	#Sécurité_physique #Gestion_des_actifs	Sécurisation des bureaux, des salles et des installations	Il convient de concevoir et de mettre en oeuvre des mesures de sécurité physique pour les bureaux, les salles et les installations.	OUI	Analyse de risques	OUI	Portes vérrouillées avec alarme en cas d'ouverture prolongée
7.4	#Sécurité_physique	Surveillance de la sécurité physique	Il convient que les locaux soient continuellement surveillés pour empêcher l'accès physique non autorisé.	OUI	Analyse de risques	OUI	Les sites de Cegid Cloud sont continuellement surveillés
7.5	#Sécurité_physique	Protection contre les menaces physiques et environnementales	Il convient de concevoir et de mettre en oeuvre une protection contre les menaces physiques et environnementales telles que les catastrophes naturelles et autres menaces physiques, intentionnelles ou non intentionnelles, impactant l'infrastructure.	OUI	Analyse de risques	OUI	Protection du bâtiment hébergeant les équipes de production Alimentation,climatisation,câblage réseau ..
7.6	#Sécurité_physique	Travail dans les zones sécurisées	Il convient que des mesures de sécurité pour le travail dans les zones sécurisées soient conçues et mises en oeuvre.	OUI	Analyse de risques	OUI	Protection du bâtiment hébergeant les équipes de production Alimentation,climatisation,câblage réseau ..
7.7	#Sécurité_physique	Bureau vide et écran vide	Il convient que des règles du bureau vide, dégagé des documents papier et des supports de stockage amovibles, et des règles de l'écran vide pour les moyens de traitement de l'information soient définies et appliquées de manière appropriée.	OUI	Analyse de risques	OUI	Politique de bureau propre - Broyeuse pour document à disposition Verouillage automatique des sessions en cas d'inactivité prolongée
7.8	#Sécurité_physique #Gestion_des_actifs	Emplacement et protection du matériel	Il convient de choisir un emplacement sécurisé pour le matériel et de le protéger.	OUI	Analyse de risques	OUI	Les matériels sensibles sont stockés dans des locaux sécurisés
7.9	#Sécurité_physique #Gestion_des_actifs	Sécurité des actifs hors des locaux	Il convient de protéger les actifs hors du site.	OUI	Analyse de risques	OUI	Chiffrement des disques, Anti Virus, connexion à distance sécurisée par passerelle d'accès et/ou VPN
7.10	#Sécurité_physique #Gestion_des_actifs	Supports de stockage	Il convient de gérer les supports de stockage tout au long de leur cycle de vie d'acquisition, d'utilisation, de transport et de mise au rebut conformément au schéma de classification et aux exigences de traitement de l'organisation.	OUI	Analyse de risques	OUI	Restriction d'utilisation des médias amovibles (USB) pour les collaborateurs Procédure fournisseur Datacenter (DC) pour les média amovibles de stockage des données clients Destruction physique des médias de stockage contenant des données client par les fournisseurs d'hébergement Chiffrement des médias de stockages amovibles en cas de transfert de données client Suivi des réceptions et des expéditions
7.11	#Sécurité_physique	Services supports	Il convient que les moyens de traitement de l'information soient protégés contre les coupures de courant et autres perturbations causées par des défaillances des services supports.	OUI	Analyse de risques	OUI	Système d'alimentation électrique indépendant est opérationnel en cas de défaillance du système général
7.12	#Sécurité_physique	Sécurité du câblage	Il convient que les câbles électriques, transportant des données ou supportant les services d'information soient protégés contre des interceptions, interférences ou dommages.	OUI	Analyse de risques	OUI	Le réseau local de la production SaaS est un réseau switché physiquement indépendant du reste de l'entreprise
7.13	#Sécurité_physique #Gestion_des_actifs	Maintenance du matériel	Il convient d'entretenir le matériel correctement pour assurer la disponibilité, l'intégrité et la confidentialité de l'information.	OUI	Analyse de risques	OUI	La maintenance des matériels internes et collaborateurs est sous traitée et contractualisée par la DSI
7.14	#Sécurité_physique #Gestion_des_actifs	Élimination ou recyclage sécurisé(e) du matériel	Il convient de vérifier les éléments du matériel contenant des supports de stockage pour s'assurer que toute donnée sensible et que tout logiciel sous licence ont été supprimés ou écrasés de façon sécurisée, avant son élimination ou sa réutilisation.	OUI	Analyse de risques	OUI	Destruction des supports contenant des données clients ou en rapport avec ces données (poste des collaborateurs)
Mesures de sécurité technologiques							
8.1	#Gestion_des_actifs #Protection_des_informations	Terminaux finaux des utilisateurs	Il convient de protéger les informations stockées, traitées ou accessibles via des terminaux finaux des utilisateurs.	OUI	Analyse de risques	OUI	Chiffrement des disques des laptops des collaborateurs Filtres de confidentialité MFA et VPN en situation de mobilité
8.2	#Gestion_des_identités_et_des_accès	Droits d'accès privilégiés	Il convient de limiter et de gérer l'attribution et l'utilisation des droits d'accès privilégiés.	OUI	Analyse de risques	OUI	Affectation des droits par groupe d'utilsateurs sur les applications à utiliser
8.3	#Gestion_des_identités_et_des_accès	Restrictions d'accès aux informations	Il convient que l'accès aux informations et autres actifs associés soit restreint conformément à la politique spécifique à la thématique du contrôle d'accès qui a été établie.	OUI	Analyse de risques	OUI	La matrice des droits et des accès définit les accès par groupe de métiers et par application
8.4	#Gestion_des_identités_et_des_accès #Sécurité_des_applications #Configuration_sécurisée	Accès aux codes source	Il convient de gérer de manière appropriée l'accès en lecture et en écriture au code source, aux outils de développement et aux bibliothèques de logiciels.	OUI	Analyse de risques	OUI	Les scripts sont stockés dans des espaces sécurisés uniquement accessibles aux equipes de production
8.5	#Gestion_des_identités_et_des_accès	Authentification sécurisée	Il convient de mettre en oeuvre des technologies et procédures d'authentification sécurisée sur la base des restrictions d'accès aux informations et de la politique spécifique à la thématique du contrôle d'accès.	OUI	Analyse de risques	OUI	La connexion des collaborateurs de Cegid Cloud aux environnements de production est effectué via un P.A.M et par un système sécurisé d'accès à distance (RDM)
8.6	#Continuité	Dimensionnement	Il convient que l'utilisation des ressources soit surveillée et ajustée selon les besoins de dimensionnement actuels et prévus.	OUI	Analyse de risques	OUI	Surveillance permanente de l'allocation des ressources Comité mensuel sur le dimensionnemnt des infrastructures et des ressources
8.7	#Sécurité_système_et_réseau #Protection_des_informations	Protection contre les programmes malveillants (malware)	Il convient qu'une protection contre les programmes malveillants soit mise en oeuvre et renforcée par une sensibilisation appropriée des utilisateurs.	OUI	Analyse de risques	OUI	Antivirus / Antimalware centralisé et administré pour toutes les ressources
8.8	#Gestion_des_menaces_et_des_vulnérabilités	Gestion des vulnérabilités techniques	Il convient d'obtenir des informations sur les vulnérabilités techniques des systèmes d'information utilisés, d'évaluer l'exposition de l'organisation à ces vulnérabilités et de prendre les mesures appropriées.	OUI	Analyse de risques	OUI	La gestion des vulnérabilité se fait par un outil de scan et par les alertes remontées par les C.E.R.T. Politique de traitement de ces vulnérabilités par périmètre en mode d'escalade Une politique de pentests et d'audit technique permet d'identifier les écarts
8.9	#Configuration_sécurisée	Gestion des configurations	Il convient que les configurations, y compris les configurations de sécurité, du matériel, des logiciels, des services et des réseaux, soient définies, documentées, mises en oeuvre, surveillées et révisées.	OUI	Analyse de risques	OUI	Durcissement des postes de travail et des serveurs
8.10	#Protection_des_informations #Réglementation_et_conformité	Suppression des informations	Il convient que les informations stockées dans les systèmes d'information, les terminaux ou tout autre support de stockage soient supprimées lorsqu'elles ne sont plus nécessaires.	OUI	Analyse de risques	OUI	Les données sensibles (données des clients, journaux) sont supprimées lorsqu'elles ne sont plus nécessaires.
8.11	#Protection_des_informations	Masquage des données	Il convient d'utiliser le masquage des données conformément à la politique spécifique à la thématique du contrôle d'accès de l'organisation et d'autres politiques spécifiques à une thématique associées, ainsi qu'aux exigences métier, tout en prenant en compte la législation applicable.	OUI	Analyse de risques	OUI	Cegid Cloud respecte les accords, lois et réglementations applicables relatives aux données à caractère personnel
8.12	#Protection_des_informations	Prévention de la fuite de données	Il convient que des mesures de prévention de la fuite de données soient appliquées aux systèmes, aux réseaux et à tous les autres terminaux qui traitent, stockent ou transmettent des informations sensibles.	OUI	Analyse de risques	OUI	Plusieurs actions et procédure permettent de prévenir la fuite de données. Exemple : la gestion d'accès à internet, la classification des données, le durcissement et chiffrement des postes de travail...
8.13	#Continuité	Sauvegarde des informations	Il convient que des copies de sauvegarde de l'information, des logiciels et des systèmes soient conservées et testées régulièrement selon la politique spécifique à la thématique de la sauvegarde qui a été convenue.	OUI	Analyse de risques	OUI	La politique de sauvegarde prend en compte la spécificité de chaque offre client. Elle prend en compte la disponibilité, l'intégrité et la rétension.
8.14	#Continuité #Gestion_des_actifs	Redondance des moyens de traitement de l'information	Il convient que les moyens de traitement de l'information soient mis en oeuvre avec suffisamment de redondance pour répondre aux exigences de disponibilité.	OUI	Analyse de risques	OUI	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
8.15	#Gestion_des_événements_de_sécurité_de_l'information	Logging	Il convient que les journaux qui enregistrent les activités, les exceptions, les pannes et autres événements pertinents soient générés, conservés, protégés et analysés.	OUI	Analyse de risques	OUI	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 L'outil de gestion de logs est hébergé dans une architecture sécurisée (redondance,chiffrement des flux et des disques, gestion des accès, sauvegarde) Un rapport l automatique des journaux administrateurs et opérateurs est produit mensuellement
8.16	#Gestion_des_événements_de_sécurité_de_l'information	Activités de surveillance	Il convient de surveiller les réseaux, systèmes et applications pour détecter les comportements anormaux et de prendre les mesures appropriées pour évaluer les éventuels incidents de sécurité de l'information.	OUI	Analyse de risques	OUI	Surveillance serveurs, postes de travail, boites mail, réseaux
8.17	#Gestion_des_événements_de_sécurité_de_l'information	Synchronisation des horloges	Il convient que les horloges des systèmes de traitement de l'information utilisés par l'organisation soient synchronisées avec des sources de temps approuvées.	OUI	Analyse de risques	OUI	Une synchronisation NTP est configurée sur tous les actifs
8.18	#Sécurité_système_et_réseau #Configuration_sécurisée #Sécurité_des_applications	Utilisation de programmes utilitaires à privilèges	Il convient que l'utilisation de programmes utilitaires ayant la capacité de contourner les mesures de sécurité des systèmes et des applications soit limitée et contrôlée étroitement.	OUI	Analyse de risques	OUI	Un outil de gestion et de limitation du shadow IT est utilisé pour contôler l'utilisation de programmes et d'appplications non autorisés

8.19	#Configuration_sécurisée #Sécurité_des_applications	Installation de logiciels sur des systèmes opérationnels	Il convient de mettre en oeuvre des procédures et des mesures pour gérer de manière sécurisée l'installation de logiciels sur les systèmes opérationnels.	OUI	Analyse de risques	OUI	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 Charte informatique
8.20	#Sécurité_système_et_réseau	Sécurité des réseaux	Il convient que les réseaux et les terminaux réseau soient sécurisés, gérés et contrôlés pour protéger les informations des systèmes et des applications.	OUI	Analyse de risques	OUI	Les réseaux et les liens sont supervisés par les outils de surveillance. Les accès sont traçés et contrôlés
8.21	#Sécurité_système_et_réseau	Sécurité des services réseau	Il convient que les mécanismes de sécurité, les niveaux de service et les exigences de services des services réseau soient identifiés, mis en oeuvre et surveillés.	OUI	Analyse de risques	OUI	Une convention de service interne est contractualisée annuellement avec la DSI Elle prend en compte la sécurité des réseaux
8.22	#Sécurité_système_et_réseau	Cloisonnement des réseaux	Il convient que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient cloisonnés dans les réseaux de l'organisation.	OUI	Analyse de risques	OUI	Cloisonnement des réseaux par la mise en place de DMZ et de VLAN.
8.23	#Sécurité_système_et_réseau	Filtrage web	Il convient que l'accès aux sites web externes soit géré pour réduire l'exposition aux contenus malveillants.	OUI	Analyse de risques	OUI	Utilisation de système de filtrage de la navigation internet
8.24	#Configuration_sécurisée	Utilisation de la cryptographie	Il convient que des règles pour l'utilisation efficace de la cryptographie, notamment la gestion des clés cryptographiques, soient définies et mises en oeuvre.	OUI	Analyse de risques	OUI	Politique édictée sur le chiffrement des flux et des données Cette politique est révisée régulièrement afin d'offrir le meilleur niveau de sécurité en adéquation avec les bonnes pratiques normalisées Administration des certificats pour accès HTTPS en accord avec les bonnes pratiques autorité de certification reconnue , stockage des clés dans un keyvault Gestion des clés de chiffrement de données stockées dans les Datacenter
8.25	#Sécurité_des_applications #Sécurité_système_et_réseau	Cycle de vie de développement sécurisé	Il convient de définir et d'appliquer des règles pour le développement sécurisé des logiciels et des systèmes.	OUI	Analyse de risques	OUI	Une politique décrit et cadre la sécurité des processus de développement
8.26	#Sécurité_des_applications #Sécurité_système_et_réseau	Exigences de sécurité des applications	Il convient que les exigences de sécurité de l'information soient identifiées, spécifiées et approuvées lors du développement ou de l'acquisition d'applications.	OUI	Analyse de risques	OUI	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 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.
8.27	#Sécurité_des_applications #Sécurité_système_et_réseau	Principes d'ingénierie et d'architecture des système sécurisés	Il convient que des principes d'ingénierie des systèmes sécurisés soient établis, documentés, tenus à jour et appliqués à toutes les activités de développement de systèmes d'information.	OUI	Analyse de risques	OUI	Les scripts et automates sont normalisés et testés avant mise en production
8.28	#Sécurité_des_applications #Sécurité_système_et_réseau	Codage sécurisé	Il convient d'appliquer des principes de codage sécurisé au développement de logiciels.	OUI	Analyse de risques	OUI	Les scripts et automates sont normalisés et testés avant mise en production Bonnes pratiques de codage sécurisé
8.29	#Sécurité_des_applications #Assurance_de_sécurité_de_l'information #Sécurité_système_et_réseau	Tests de sécurité dans le développement et l'acceptation	Il convient que des processus pour les tests de sécurité soient définis et mis en oeuvre au cours du cycle de vie de développement.	OUI	Analyse de risques	OUI	Les phases de test et les tests de conformité sont assurés dans le workflow AzureDevOps
8.30	#Sécurité_système_et_réseau #Sécurité_des_applications #Sécurité_des_relations_fournisseurs	Développement externalisé	Il convient que l'organisation dirige, contrôle et vérifie les activités relatives au développement externalisé des systèmes.	OUI	Analyse de risques	OUI	Une convention de service interne avec les BU de développement supervise et contôle les activités et applications externes au SMSI
8.31	#Sécurité_des_applications #Sécurité_système_et_réseau	Séparation des environnements de développement, de test et opérationnels	Il convient de séparer et de sécuriser les environnements de développement, de test et opérationnels.	OUI	Analyse de risques	OUI	Segrégation assurée par le workflow automatisé par une organisation de type DevOps
8.32	#Sécurité_des_applications #Sécurité_système_et_réseau	Gestion des changements	Il convient que les changements apportés aux moyens de traitement de l'information et aux systèmes d'information soient soumis à des procédures de gestion des changements.	OUI	Analyse de risques	OUI	Les changements standards sont opérés via le workflow de l'orchestrateur de la plateforme. Les changements non standard sont traités par le processus de change Les mises à jour matériel et/ou système sont testés sur des groupes pilotes avant application sur les environnements de production Tous les changements relatifs aux scrips et automates sont consignés dans un git
8.33	#Protection_des_informations	Informations de test	Il convient que les informations de test soient sélectionnées, protégées et gérées de manière appropriée.	OUI	Analyse de risques	OUI	Gérer par le workflow AzureDevOps et les serveurs de développement
8.34	#Sécurité_système_et_réseau #Protection_des_informations	Protection des systèmes d'information pendant les tests d'audit	Il convient que les tests d'audit et autres activités d'assurance impliquant l'évaluation des systèmes opérationnels soient planifiés et convenus entre le testeur et le niveau approprié du management.	OUI	Analyse de risques	OUI	Les différentes politiques (Scan) et accords (Pentest) prennent en compte les périodes d'activités des métiers afin de minimiser les impacts