Catalogue des mesures de cybersécurité du service « Tester avant d'investir » [1]

La durée de chaque mission subventionnée pour la mise en œuvre d'une ou plusieurs mesures ne pourra excéder 14 jours et devra être un multiple de 0,5 jour.

Les taux journaliers moyens (TJM) devront être compris entre 400 et 800 € H.T.

Dans la limite des durées de mission et des TJM indiqués ci-dessus, les prestataires retenus disposeront d'une libre appréciation pour définir la durée et le prix de chaque mesure.

Cependant, pour chaque mesure, ce catalogue propose une **Durée estimée** et un **TJM préconisé**.

Exemple :

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 5	3 à 6	4 à 8
TJM préconisé	Profil : Consultant → 800€/j			

Attention :

Ce **pictogramme** indique que pour prétendre réaliser cette mesure, les intervenants du prestataire doivent indiquer disposer d'une certification technique de l'éditeur ou du constructeur sur la technologie à intégrer.
OU indiquer 3 références de moins de 3 ans sur des projets et bénéficiaires similaires.

Ce **pictogramme** indique que pour prétendre réaliser cette mesure, les intervenants du prestataire doivent disposer d'une certification de DPO.
OU indiquer 3 références de moins de 3 ans sur des projets et bénéficiaires similaires.

[1] Catalogue réalisé dans le cadre du Module de travail n°4 de l'EDIH La Réunion, en charge du service « Tester avant d'investir »

0. Référentiel des mesures

Gouvernance :

Etablir la liste des activités métiers et des données à protéger en priorité (essentielles, sensibles, critiques)	GOUV_01	Fiche n°1
Disposer d'un schéma global (à jour) du **réseau informatique** et des interconnexions	GOUV_02	Fiche n°2
Disposer d'un schéma global (à jour) du **réseau industriel** et des interconnexions	GOUV_02_b	Fiche n°2_bis
Fixer des exigences de cybersécurité aux prestataires du **réseau informatique**	GOUV_03	Fiche n°3
Fixer des exigences de cybersécurité aux prestataires du **réseau industriel**	GOUV_3_b	Fiche n°3_bis
Etablir la liste des données personnelles traitées au sein de votre entité	GOUV_04	Fiche n°4
Fournir des informations aux personnes concernées sur l'utilisation de leurs données personnelles	GOUV_05	Fiche n°5

Sécurité des postes :

Installer de manière systématique un antivirus sur les **postes de travail du SI bureautique**, vérifier régulièrement leur bon fonctionnement et leurs maj.	SEC_POS_01	Fiche n°6
Installer de manière systématique un antivirus sur les **postes de travail du SI Industriel**, vérifier régulièrement leur bon fonctionnement et leurs maj.	SEC_POS_01_b	Fiche n°6 bis
Activer systématiquement le pare-feu local sur les postes de travail avec comme règle générale d'interdire par défaut les flux entrants.	SEC_POS_02	Fiche n°7
Déployer systématiquement toutes les mises à jour dès que celles-ci sont disponibles (ou après qualification interne) et hors exceptions spécifiquement identifiées, sur le **SI bureautique**	SEC_POS_03	Fiche n°8
Déployer systématiquement toutes les mises à jour dès que celles-ci sont disponibles (ou après qualification interne) et hors exceptions spécifiquement identifiées, sur le **SI industriel**	SEC_POS_03_b	Fiche n°8_bis

Mettre en œuvre une solution de type EDR (Endpoint Detection & Response)	SEC_POS_04	Fiche n°9
Chiffrer les disques durs des matériels nomades	SEC_POS_05	Fiche n°10

Sécurité des infrastructures :

Déployer systématiquement toutes les mises à jour dès que celles-ci sont disponibles (ou après qualification interne) et hors exceptions spécifiquement identifiées, sur **le SI bureautique**	SEC_INF_01	Fiche n°11
Déployer systématiquement toutes les mises à jour dès que celles-ci sont disponibles (ou après qualification interne) et hors exceptions spécifiquement identifiées, sur le **SI industriel**	SEC_INF_01_b	Fiche n°11 bis
Fermer tous les flux et les ports non strictement nécessaires	SEC_INF_02	Fiche n°12
Activer et conserver l'historique de l'ensemble des flux bloqués et des flux entrants et sortants identifiés par le pare-feu	SEC_INF_03	Fiche n°13
Déployer un pare-feu physique en mettant en place les cloisonnements suivants : - Fermer tous les flux et ports non strictement nécessaires. - Activer et conserver l'historique de l'ensemble des flux bloqués et des flux entrants et sortants identifiés par le pare-feu	SEC_INF_04	Fiche n°14
Déployer un pare-feu physique pour cloisonner le **réseau industriel** du **réseau bureautique** : - Fermer tous les flux et ports non strictement nécessaires. - Activer et conserver l'historique de l'ensemble des flux bloqués et des flux entrants et sortants identifiés par le pare-feu	SEC_INF_04_b	Fiche n°14 bis
Mettre en œuvre une solution d'anti-spam et d'anti-hameçonnage	SEC_INF_05	Fiche n°15
Recourir au chiffrement robuste du Wi-Fi	SEC_INF_06	Fiche n°16
Protéger l'accès à l'espace de stockage des serveurs et des équipements réseau par une porte pouvant être fermée à clef	SEC_INF_07	Fiche n°17

Sécurité des accès :

Limiter drastiquement le nombre d'utilisateurs disposant du privilège d'administration local sur leur machine.	SEC_ACC_01	Fiche n° 18
Utiliser des comptes d'administration dédiées à cet usage, les administrateurs disposant en parallèle d'un compte utilisateur. Utiliser également des comptes d'administration distincts dédiés à l'administration de l'AD/Samba-AD et à la solution de sauvegarde (et non géré via l'AD/Samba-AD).	SEC_ACC_02	Fiche n°19
Mettre en place selon les possibilités, un mécanisme d'authentification multifacteur pour accéder aux comptes d'administration et à hauts privilèges ainsi que des contraintes renforcées de robustesse et de longueur de mots de passe (15 caractères minimum)	SEC_ACC_03	Fiche n°20
Mettre en place pour tous les accès distants des mécanismes d'authentification multifacteur à minima, avec restriction via adresses IP (ex : localisation, pays, plages horaires)	SEC_ACC_04	Fiche n°21
Mettre en place pour tous les accès distants du **SI industriel** des mécanismes d'authentification multifacteur à minima, avec restriction via adresses IP (ex : localisation, pays, plages horaires)	SEC_ACC_04_b	Fiche n°21 bis
Restreindre l'accès aux données à protéger en priorité aux seules personnes autorisées à y accéder (ex : un tableau répertoriant les utilisateurs légitimes par systèmes/applications à protéger en priorité)	SEC_ACC_05	Fiche n°22
Fixer des contraintes de longueur et de complexité des mots de passe exigeant à minima 12 caractères incluant minuscules, majuscules, chiffres et caractères spéciaux, 16 caractères pour les utilisateurs détenant les droits d'administration local de leur poste de travail.	SEC_ACC_06	Fiche n°23
Réaliser **annuellement** une revue des accès utilisateurs en les comparant avec les informations détenues par le service RH. Les mots de passes des comptes partagés concernés sont renouvelés à chaque départ.	SEC_ACC_07	Fiche n°24
Réaliser tous les **6 mois** une revue des accès administrateurs en les comparant avec les informations détenues par le service RH. Les mots de passes des comptes partagés concernés sont renouvelés à chaque départ.	SEC_ACC_07_b	Fiche n°24 bis
Mettre en place selon les possibilités, un mécanisme d'authentification multifacteur pour accéder aux données jugées les plus sensibles et/ou des contraintes renforcées de robustesse et de longueur de mots de passe (15 caractères minimum)	SEC_ACC_08	Fiche n°25

Mettre en œuvre un outil de gestion des politiques de sécurité centralisé (ex : Active Directory, Samba-AD) et en évaluer/améliorer son niveau de sécurité annuellement, idéalement au travers d'un accompagnement extérieur.	SEC_ACC_09	Fiche n°26

Réaction à une cyberattaque :

Réaliser des sauvegardes régulières autant que de besoin et dont le rythme est jugé acceptable par le CODIR.	REAC_INC_01	Fiche n°27
Procéder régulièrement à des tests de restauration des données critiques qui sont stockées dans un environnement sécurisé et isolée d'internet, à minima une fois par semestre	REAC_INC_02	Fiche n°28
Disposer d'une sauvegarde des données critiques stockées dans un environnement sécurisé, isolé de l'environnement bureautique et d'internet, en complément des sauvegardes régulièrement réalisées et stockées sur le réseau (ex : sauvegarde amovible, hors AD, cloud privé, solution de sauvegarde externalisée dédiée). Déterminer le rythme de sauvegarde avec le CODIR.	REAC_INC_03	Fiche n°29
Lister les personnes à contacter en cas d'incident de sécurité informatique	REAC_INC_04	Fiche n°30
Réaliser une veille trimestrielle sur internet (ex : veille des avis et alertes publiés sur le site du CERT-FR)	REAC_INC_05	Fiche n°31

Sensibilisation des utilisateurs :

Encourager régulièrement (2 fois par an à minima) la déclaration d'incident auprès de vos agents en rappelant les évènements "signaux faibles" devant être signalés ainsi que le contact à alerter. Formaliser et diffuser une fiche réflexe dédiée aux utilisateurs.	SENS_UTIL_01	Fiche n°32
Etablir une charte informatique répertoriant les moyens informatiques mis à disposition, clarifiant la gestion des terminaux personnels et rappelant à minima les exigences de cybersécurité liées à la gestion des comptes d'accès, des mots de passe, des données à protéger en priorités, de l'utilisation de la messagerie et des ressources cloud.	SENS_UTIL_02	Fiche n°33

1. Définir une gouvernance

La gouvernance en cybersécurité désigne l'ensemble des principes, politiques et processus mis en place pour garantir une gestion cohérente, efficace et proactive des risques liés à la sécurité numérique. Elle implique de définir des responsabilités claires, d'élaborer des stratégies adaptées et de s'assurer de leur mise en œuvre dans toute l'organisation.

La gouvernance constitue le socle de la sécurité des systèmes d'information : sans elle, les efforts de protection et de réaction sont souvent mal coordonnés, inefficaces ou sous-optimisés.

Un manque de gouvernance peut conduire à :

- Une vision floue des responsabilités et priorités en matière de cybersécurité.
- Des investissements non ciblés et inefficaces.
- Une réactivité insuffisante face aux menaces et incidents.

En revanche, une gouvernance bien structurée permet de poser des bases solides pour protéger efficacement les actifs critiques et garantir la continuité des activités en cas de cyberattaque.

1. Centralisation et clarté : Identifier clairement qui est responsable de quoi, et éviter les doublons ou oublis.
2. Décisions éclairées : Prioriser les actions de cybersécurité en fonction des risques réels et des ressources disponibles.
3. Conformité légale : Répondre aux exigences réglementaires en matière de protection des données (ex. RGPD).
4. Confiance accrue : Renforcer la crédibilité auprès des clients, partenaires et fournisseurs en démontrant un engagement actif en matière de cybersécurité.
5. Réduction des coûts : Optimiser les budgets en alignant les investissements sur les priorités stratégiques.

En résumé, la gouvernance en cybersécurité n'est pas réservée aux grandes entreprises : elle est essentielle, même pour les TPE et PME. En adoptant des mesures simples mais structurées, ces organisations peuvent poser les bases d'une défense efficace contre les menaces numériques tout en maximisant la valeur de leurs efforts et ressources.

Fiche-Action n°1 : Établir la liste des activités et des données à protéger en priorité

Description	Mesure qui permet de remettre au centre de la démarche de sécurisation les véritables enjeux de sécurité de l'entité et de prioriser les efforts de sécurisation « au bon endroit ».
Phases du projet	La liste des activités (métiers) et des informations est établie de manière collective, au cours d'un atelier de réflexion impliquant les directions métiers et/ou les décideurs de l'organisation. Lister les lieux de stockage de ces informations, quelles sont les personnes qui y accèdent, et comment elles sont sauvegardées.
Méthodologie	Chaque contributeur réfléchi aux activités et/ou données qui semblent essentielles à la continuité des missions de l'organisation, et qui par conséquent, ne peuvent être indisponibles, altérés ou volées/divulguées. Ces réflexions sont présentées, et font l'objet d'une validation commune.
Prérequis pour l'entreprise	Disponibilité des parties prenantes et accès aux documents et données nécessaires pour évaluation.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 3	3 à 4	3 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Identification des priorités stratégiques grâce à la découverte de la criticité des informations. Optimisation des ressources afin de protéger efficacement les données. Un premier pas vers la conformité réglementaire (RGPD), en identifiant les données personnelles sensibles. Implication de la direction et des métiers dans la protection du patrimoine informationnel. Renforcement de la résilience car cette liste apporte une vision structurée et stratégique en cas de réponse à incident.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Une liste détaillée des activités et des données critiques associées, accompagnée d'une matrice des priorités (criticité, impact, responsables...). Une brève synthèse des risques associés. Un plan d'actions prioritaires pour protéger ces informations.

Fiche-Action n°2 : Disposer d'un schéma global (à jour) du réseau informatique et de la liste des interconnexions vers l'extérieur.

Description	L'objectif de cette mesure est de cartographier l'ensemble du réseau informatique de l'entreprise, y compris ses interconnexions vers l'extérieur (Internet, réseaux partenaires ou prestataires), afin de mieux comprendre son architecture, identifier les vulnérabilités potentielles et sécuriser les points d'accès critiques.
Phases du projet	Préparation : analyse des documents disponibles. Inventaire : identification des actifs présents et des interconnexions vers l'extérieur. Cartographie : création d'un schéma des segments réseaux, des relations inter-équipements et points d'interconnexion. Flux : analyse des flux entrants/sortants autorisés. Rédaction : Formalisation des éléments collectés pour mise à jour de la documentation.
Méthodologie	Approche basée sur l'analyse de risques, les standards ISO 27001 et de façon plus globale sur les bonnes pratiques cyber.
Prérequis pour l'entreprise	Préparation de la documentation existante, implication des responsables IT et des prestataires, accès aux infrastructures.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 3	3 à 4	3 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Une vision claire de l'architecture des réseaux. Une détection anticipée des possibles points de vulnérabilité, diminuant ainsi l'exposition aux risques, tout en optimisant les efforts de sécurisation sur les points les plus sensibles. Une meilleure efficacité opérationnelle.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport de mission synthétique. Schéma global du réseau incluant les interconnexions vers l'extérieur. Procédure de mise à jour de la cartographie (selon le temps disponible).

Fiche-Action n°2_bis : Disposer d'un schéma global (à jour) du réseau industriel et de la liste des interconnexions vers l'extérieur

Description	L'objectif de cette mesure est de cartographier l'ensemble du réseau industriel de l'entreprise, y compris ses interconnexions vers l'extérieur (Internet, réseaux partenaires ou prestataires), afin de mieux comprendre son architecture, identifier les vulnérabilités potentielles et sécuriser les points d'accès critiques (capteurs, actionneurs, automates, IoT, etc.).
Phases du projet	Préparation : analyse des documents disponibles. Inventaire : identification des actifs industriels présents et des interconnexions vers l'extérieur Cartographie : création d'un schéma des segments réseaux, des relations inter-équipements et points d'interconnexion. Flux : analyse des flux entrants/sortants autorisés. Rédaction : Formalisation des éléments collectés pour mise à jour de la documentation.
Méthodologie	Approche basée sur l'analyse de risques, les standards ISO 27001 et de façon plus globale sur les bonnes pratiques cyber.
Prérequis pour l'entreprise	Préparation de la documentation existante, implication des responsables IT et des prestataires, accès aux infrastructures.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	3 à 4	3 à 4	4 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Une vision claire de l'architecture des réseaux industriels. Une détection anticipée des possibles points de vulnérabilité, diminuant ainsi l'exposition aux risques, tout en optimisant les efforts de sécurisation sur les points les plus sensibles. Une meilleure efficacité opérationnelle.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport de mission synthétique. Schéma global du réseau industriel incluant les interconnexions vers l'extérieur. Procédure de mise à jour de la cartographie (selon le temps disponible).

Fiche-Action n°3 : Fixer des exigences de cybersécurité aux prestataires du réseau informatique

Description	Mesure consistant à ajouter des exigences de sécurité dans les contrats de prestation, pour responsabiliser les prestataires du réseau informatique et leurs personnels vis-à-vis de votre entité. Cibles de choix et faisant l'objet de toutes les attentions ces dernières années, les prestataires (supply chain) sont des points d'entrée « autorisés » vers votre SI.
Phases du projet	Préparation : inventaire et analyse des contrats de prestation en cours (et à venir). Analyse : identification des écarts avec vos règles et vos mesures de sécurité. Rédaction : propositions de correctifs ou d'ajouts aux contrats de prestation en cours, à diffuser après de vos prestataires.
Méthodologie	Approche basée sur le modèle de l'analyse de risques, les standards ISO 27001 et les recommandations du RGPD. Les exigences sont adaptées à la maturité, et aux moyens de l'organisation.
Prérequis pour l'entreprise	Implication de la direction, des responsables IT et des prestataires.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 5	3 à 6	4 à 8
TJM préconisé	Profil : Consultant → 800€/j			

Valeur ajoutée	Une connaissance pointue des limites des contrats de prestation. Une propagation de vos exigences de sécurité à vos partenaires. La prise en compte de bonnes pratiques en termes d'hygiène informatique. Une protection supplémentaire en cas de recours juridique suite à un incident.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Liste (à jour) des contrats de prestation en cours (et à venir). Matrice des contrats à risque (dépendances/risques/criticités). Propositions de modifications/ajouts aux divers contrats concernés.

Fiche-Action n°3_bis : Fixer des exigences de cybersécurité aux prestataires du réseau industriel

Description	Mesure consistant à ajouter d'exigences de sécurité dans les contrats de prestation, pour responsabiliser les prestataires du réseau industriel et leurs personnels vis-à-vis de votre entité. Cibles de choix et faisant l'objet de toutes les attentions ces dernières années, les prestataires (supply chain) sont des points d'entrée « autorisés » vers votre SI.
Phases du projet	Préparation : inventaire et analyse des contrats de prestation en cours (et à venir). Analyse : identification des écarts avec vos règles et vos mesures de sécurité. Rédaction : propositions de correctifs ou d'ajouts aux contrats de prestation en cours, à diffuser après de vos prestataires.
Méthodologie	Approche basée sur le modèle de l'analyse de risques, les standards ISO 27001 et les recommandations du RGPD. Les exigences sont adaptées à la maturité, et aux moyens de l'organisation.
Prérequis pour l'entreprise	Implication de la direction, des responsables IT et des prestataires.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 5	3 à 6	4 à 8
TJM préconisé	Profil : Consultant → 800€/j			

Valeur ajoutée	Une connaissance pointue des limites des contrats de prestation. Une propagation de vos exigences de sécurité à vos partenaires. La prise en compte de bonnes pratiques en termes d'hygiène informatique. Une protection supplémentaire en cas de recours juridique suite à un incident.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Liste (à jour) des contrats de prestation en cours (et à venir). Matrice des contrats à risque (dépendances/risques/criticités). Propositions de modifications/ajouts aux divers contrats concernés.

Fiche-Action n°4 : Etablir la liste des données personnelles traitées au sein de votre entité

Description	Mesure consistant à cartographier les données personnelles traitées par l'entreprise ou la collectivité, car la protection des données personnelles est une obligation légale imposée par le RGPD.
Phases du projet	Préparation : identification des types de données personnelles collectées par l'entreprise (identification, professionnelles, financières, commerciales, sensibles...). Recensement des traitements associés à ces données (pourquoi, par qui, où, quand, comment…) Mise en œuvre : identification des traitements non-conformes, analyse d'impact, chiffrement et limitation des accès. Rédaction : formalisation d'un registre des traitements.
Méthodologie	Approche basée sur le modèle d'un diagnostic RGPD, en s'appuyant sur les recommandations de la CNIL pour la mise en œuvre.
Prérequis pour l'entreprise	Implication de la direction, des responsables métiers et de l'IT. Accès aux bases de données et outils contenant des données personnelles. Accès aux contrats avec les sous-traitants manipulant ces données. Nomination d'un référent : Responsable des traitements ou DPO

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 5	6 à 10	8 à 14	8 à 14
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	1er pas essentiel vers la conformité au RGPD. Réduction des risques juridiques. Meilleure maitrise de la sécurisation des données personnelles et sensibles Optimisation des processus de gestion des données personnelles. Renforcement de la confiance des clients et partenaires.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Listes des traitements de données personnelles Amorce de registre des traitements. Plan de sécurisation des données personnelles. Procédure de mise à jour du document.

Fiche-Action n°5 : Fournir des informations aux personnes concernées sur l'utilisation de leurs données personnelles

Description	Mesure consistant à se conformer au RGPD en termes de transparence sur l'utilisation des données personnelles qui sont collectées par l'entreprise ou la collectivité.
Phases du projet	Préparation : identification des points de collectes des données personnelles (formulaires, cookies, RH, vidéosurveillance...) Rédaction : rédaction de la politique de confidentialité et des mentions légales, mise à jour des documents contractuels et des supports d'information, processus de réponse aux demandes d'information des personnes concernées.
Méthodologie	Approche basée sur le modèle d'un diagnostic RGPD, en s'appuyant sur les recommandations de la CNIL pour la mise en œuvre.
Prérequis pour l'entreprise	Implication de la direction, des responsables métiers et de l'IT. Accès au registre des traitements, ou à la liste des données personnelles. Accès aux documents juridiques et aux supports d'information. Nomination d'un référent : Responsable des traitements ou DPO

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 5	6 à 10	10 à 14	10 à 14
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	1er pas essentiel vers la conformité au RGPD. Réduction des risques juridiques. Amélioration de l'image de l'entreprise ou la collectivité. Optimisation des processus de gestion des demandes. Renforcement de la confiance des clients et partenaires.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Politique de confidentialité et des mentions légales conformes. Procédure de gestion interne des demandes des personnes concernées.

2. Sécuriser les postes clients (et nomades)

Les postes clients (PC fixes, portables, tablettes, smartphones) représentent aujourd'hui le premier point d'entrée des cyberattaques. Ils sont utilisés quotidiennement pour accéder aux emails, aux applications métiers et aux données sensibles. Un poste mal protégé peut être compromis par des logiciels malveillants, des attaques par hameçonnage ou des failles non corrigées.

La sécurisation des postes clients repose sur plusieurs mesures essentielles, telles que la gestion des mises à jour, le déploiement d'antivirus et d'outils de détection, la protection des accès ou encore le chiffrement des disques durs.

Ce volet propose un ensemble de solutions concrètes pour protéger vos collaborateurs et leurs outils de travail tout en limitant votre exposition à des risques majeurs tels que :

- Le vol ou la perte de données sensibles via des logiciels malveillants ou du phishing.
- La propagation de virus et ransomwares à l'ensemble du réseau.
- Les intrusions non autorisées si les identifiants des utilisateurs sont compromis.
- Les dégradations des performances et interruptions d'activité suite à des infections.

En résumé, la sécurité des postes de travail est un pilier fondamental de la cybersécurité. Les entreprises, même de petite taille, doivent mettre en place des protections simples mais efficaces, afin de réduire leur exposition aux menaces et garantir la continuité des activités.

Fiche-Action n°6 : Installer de manière systématique un antivirus sur les postes de travail bureautique.

Description	Mesure en faveur du déploiement de solutions antivirus et anti-malware pour détecter automatiquement et prévenir les menaces informatiques en temps réel.
Phases du projet	Préparation : Identification des postes de travail concernés. Analyse : Sélection des solutions adaptées en fonction des besoins de l'entreprise. Mise en œuvre : Installation, configuration, activation du Firewall local et lancement d'un premier scan complet des postes. Restitution : Rapport des configurations et recommandations pour la maintenance.
Méthodologie	Utilisation de solutions reconnues sur le marché pour leur protection efficace en temps réel. Déploiement initial en environnement pilote avant la généralisation. Transfert de compétences aux utilisateurs et responsables IT pour une exploitation optimale de la solution. Assistance technique pour les mises à jour et la maintenance.
Prérequis pour l'entreprise	Inventaire des équipements bureautiques à protéger. Accès aux configurations réseaux et serveurs.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	3 à 5	3 à 5
TJM préconisé	Profil : Technicien/Admin → 400€/j			

Valeur ajoutée	Protection proactive contre les menaces informatiques. Réduction des risques d'infections virales et d'interruptions de service.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Solutions antivirus et anti-malware opérationnelles. Rapport détaillé des installations et configurations. Rapport synthétique du 1er scan des postes.

Fiche-Action n°6_bis : Installer de manière systématique un antivirus sur les postes de travail industriels.

Description	Mesure en faveur du déploiement de solutions antivirus et anti-malware pour détecter automatiquement et prévenir les menaces informatiques en temps réel.
Phases du projet	Préparation : Identification des postes de travail industriels concernés. Analyse : Sélection des solutions adaptées en fonction des besoins de l'entreprise. Mise en œuvre : Installation, configuration, activation du Firewall local et lancement d'un premier scan complet des postes. Restitution : Rapport des configurations et recommandations pour la maintenance.
Méthodologie	Utilisation de solutions reconnues sur le marché pour leur protection efficace en temps réel. Déploiement initial en environnement pilote avant la généralisation. Transfert de compétences aux utilisateurs et responsables IT pour une exploitation optimale de la solution. Assistance technique pour les mises à jour et la maintenance.
Prérequis pour l'entreprise	Inventaire des équipements industriels à protéger. Accès aux configurations réseaux et serveurs.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	3 à 5	3 à 5
TJM préconisé	Profil : Technicien/Admin → 400€/j			

Valeur ajoutée	Protection proactive contre les menaces informatiques. Réduction des risques d'infections virales et d'interruptions de service.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Solutions antivirus et anti-malware opérationnelles. Rapport détaillé des installations et configurations. Rapport synthétique du 1er scan des postes.

Fiche-Action n°7 : Activer systématiquement le pare-feu local sur les postes de travail avec comme règle générale d'interdire par défaut les flux entrants.

Description	Mesure permettant de limiter l'exposition des postes de travail, en n'autorisant que les connexions sortantes nécessaires aux usages métiers.
Phases du projet	Préparation : Identification des postes de travail concernés, et vérification de leur configuration actuelle. Analyse : Recensement des exceptions métiers nécessaires, et validation des règles avec les équipes IT. Mise en œuvre : Activation du Firewall local, application de la politique de blocage des flux entrants et ajouts des exceptions. Restitution : Rapport des configurations et recommandations pour la maintenance.
Méthodologie	Application calquée selon les standards de sécurité actuels. Déploiement initial en environnement pilote avant la généralisation. Transfert de compétences au responsable IT pour maintenance.
Prérequis pour l'entreprise	Inventaire des équipements concernés. Inventaire des applications nécessitant des flux entrants légitimes. Accès aux outils de gestion centralisée des postes (si existants)

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	3 à 5	3 à 5
TJM préconisé	Profil : Technicien/Admin → 400€/j			

Valeur ajoutée	Protection proactive contre les menaces informatiques. Réduction des risques d'attaque réseau. Conformité aux standards de sécurité Renforcement de la sécurité sans impact sur l'usage quotidien. Gestion centralisée et évolutive.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Pare-feu activé sur tous les postes de travail. Rapport détaillé des configurations et règles appliquées.

Fiche-Action n°8 : Déployer systématiquement les mises à jour sur les postes de travail bureautiques

Description	Cette mesure a pour objectif de renforcer la sécurité des postes de travail en assurant la mise à jour régulière des systèmes d'exploitation et des logiciels. Elle vise à protéger les équipements contre les cybermenaces en corrigeant rapidement les vulnérabilités connues et exploitables.
Phases du projet	Préparation : Identification des postes de travail bureautiques concernés et des outils de gestion disponibles. Analyse : Évaluation de l'état actuel des postes (mises à jour, antivirus, droits d'accès). Mise en œuvre : Installation des mises à jour nécessaires et configuration des outils de sécurité (maj auto). Restitution : Rapport des actions réalisées et recommandations pour le maintien de la sécurité.
Méthodologie	Utilisation des outils de gestion centralisée pour les mises à jour et la sécurité (ex : WSUS, SCCM). Application conforme des recommandations des éditeurs et des standards internationaux (ex : ANSSI). Transfert de compétences aux utilisateurs et responsables IT.
Prérequis pour l'entreprise	Liste des postes de travail bureautiques concernés avec leur configuration actuelle. Disponibilité des responsables IT pour la coordination. Accès aux outils de gestion centralisée des postes (si existants)

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction des risques liés aux cyberattaques grâce à des mises à jour régulières. Renforcement de la productivité grâce à des postes de travail mieux sécurisés. Conformité avec les standards en matière de sécurité.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Rapport détaillé des mises à jour réalisées Plan de maintenance pour la gestion continue des postes de travail.

Fiche-Action n°8_bis : Déployer systématiquement les mises à jour sur les postes de travail industriels

Description	Cette mesure a pour objectif de renforcer la sécurité des postes de travail industriels en assurant la mise à jour régulière des systèmes d'exploitation et des logiciels. Elle vise à protéger les équipements contre les cybermenaces en corrigeant rapidement les vulnérabilités connues et exploitables.
Phases du projet	Préparation : Identification des postes de travail industriels concernés et des outils de gestion disponibles. Analyse : Évaluation de l'état actuel des postes (mises à jour, antivirus, droits d'accès). Mise en œuvre : Installation des mises à jour nécessaires et configuration des outils de sécurité (maj auto). Restitution : Rapport des actions réalisées et recommandations pour le maintien de la sécurité.
Méthodologie	Utilisation des outils de gestion centralisée pour les mises à jour et la sécurité (ex : WSUS, SCCM). Application conforme des recommandations des éditeurs et des standards internationaux (ex : ANSSI). Transfert de compétences aux utilisateurs et responsables IT.
Prérequis pour l'entreprise	Liste des postes de travail industriels concernés avec leur configuration actuelle. Disponibilité des responsables IT pour la coordination. Accès aux outils de gestion centralisée des postes (si existants)

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction des risques liés aux cyberattaques grâce à des mises à jour régulières. Renforcement de la productivité grâce à des postes de travail industriels mieux sécurisés. Conformité avec les standards en matière de sécurité.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Rapport détaillé des mises à jour réalisées Plan de maintenance pour la gestion continue des postes industriels.

Fiche-Action n°9 : Mettre en œuvre une solution de type EDR (EndPoint Detection & Response)

Description	Mesure visant à installer et configurer une solution EDR pour surveiller, détecter et répondre aux menaces sur tous les postes de travail.
Phases du projet	Préparation : Identification des postes de travail à protéger et choix de la solution EDR qu'ils soient bureautiques et/ou industriels. Analyse : Évaluation de la compatibilité des systèmes et du paramétrage initial nécessaire. Mise en œuvre : Installation et tests de la solution sur les postes sélectionnés. Restitution : Rapport des configurations et recommandations.
Méthodologie	Déploiement d'une solution EDR fiable et reconnue pour son efficacité. Configuration initiale pour maximiser les capacités de détection. Transfert de compétences aux utilisateurs et responsables IT pour une exploitation optimale de la solution.
Prérequis pour l'entreprise	Liste des postes à protéger et leur configuration existante. Accès aux systèmes pour l'installation.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Surveillance proactive et réponse rapide aux incidents. Amélioration de la sécurité globale des postes de travail.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Solution EDR déployée sur les postes sélectionnés. Rapport des configurations et guide d'utilisation.

Fiche-Action n°10 : Chiffrer les disques durs des matériels nomades

Description	L'objectif est de sécuriser les données stockées sur les équipements mobiles (PC portables, smartphones, disques externes, clés USB) en activant le chiffrement des disques durs. Cette mesure empêche l'accès aux informations en cas de perte ou de vol du matériel, protégeant ainsi les données sensibles contre toute tentative d'exploitation malveillante.
Phases du projet	Préparation : Identification des postes nomades à protéger et choix de la solution de chiffrement. Analyse : évaluation de la compatibilité des postes concernés. Mise en œuvre : Activation et configuration du chiffrement Test : Vérification du bon chiffrement et simulation de récupération de données avec la clé de chiffrement. Restitution : Rapport des configurations et recommandations.
Méthodologie	Déploiement d'une solution de chiffrement reconnue pour sa robustesse et sa simplicité d'utilisation. Configuration optimale limitant les ralentissements. Choix d'une politique de gestion des clés. Transfert de compétences aux utilisateurs et responsables IT pour une meilleure exploitation de la solution.
Prérequis pour l'entreprise	Liste des postes à protéger et configurations existantes. Définition des responsables de la gestion des clés. Accès aux systèmes pour l'installation.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	3 à 6	4 à 8	4 à 8
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Protection des données sensibles en cas de vol ou perte. Point de conformité aux réglementations, cette mesure aide à respecter certaines obligations légales (ex. RGPD, NIS…) Réduction du risque de fuite d'informations. Sécurité accrue pour les personnels en mobilité, idéal pour les salariés en télétravail, les consultants, commerciaux, et surtout les dirigeants.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de mission. Liste des équipements protégés, et politique de chiffrement adoptée. Rapport des configurations et guide d'utilisation.

3. Sécuriser les infrastructures

Les infrastructures informatiques regroupent l'ensemble des équipements réseau et systèmes qui assurent le bon fonctionnement du système d'information d'une entreprise : serveurs, équipements réseau (routeurs, switches, pare-feu), systèmes de stockage locaux et solutions cloud.

Ces composants sont essentiels pour garantir la disponibilité, l'intégrité et la confidentialité des données et services numériques. Une infrastructure mal protégée peut devenir une cible privilégiée pour les cyberattaques, entraînant des interruptions de service, des fuites de données ou des compromissions du réseau.

Une infrastructure non-sécurisée expose l'entreprise à des risques majeurs tels que :

- Les intrusions et piratages via des équipements mal configurés ou obsolètes.
- Les attaques par ransomware pouvant chiffrer l'ensemble des données stockées.
- L'exfiltration de données sensibles si les accès au réseau ne sont pas maîtrisés.
- L'arrêt total de l'activité en cas d'attaque ciblant des services critiques.

En résumé, la sécurité des infrastructures est un élément clé de la cybersécurité. Une bonne protection des équipements et des réseaux limite les vulnérabilités et réduit l'impact des cyberattaques.

Même avec des moyens limités, les TPE et PME peuvent mettre en place des mesures simples mais efficaces pour renforcer leur résilience face aux cybermenaces.

Fiche-Action n°11 : Déployer systématiquement les mises à jour sur les serveurs du SI bureautique

Description	Cette mesure a pour objectif de renforcer la sécurité des serveurs bureautique en assurant la mise à jour régulière des systèmes d'exploitation et des logiciels. Elle vise à protéger les équipements contre les cybermenaces en corrigeant rapidement les vulnérabilités connues et exploitables.
Phases du projet	Préparation : Identification des serveurs bureautique concernés et des outils de gestion disponibles. Analyse : Évaluation de l'état actuel des serveurs (mises à jour, antivirus, droits d'accès). Mise en œuvre : Installation des mises à jour nécessaires et configuration des outils de sécurité (maj auto). Restitution : Rapport des actions réalisées et recommandations pour le maintien de la sécurité.
Méthodologie	Utilisation des outils de gestion centralisée pour les mises à jour et la sécurité (ex : WSUS, SCCM). Application conforme des recommandations des éditeurs et des standards internationaux (ex : ANSSI).
Prérequis pour l'entreprise	Liste des serveurs concernés avec leur configuration actuelle. Disponibilité des responsables IT pour la coordination.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction des risques liés aux cyberattaques grâce à des maj régulières. Renforcement de la productivité grâce à des serveurs mieux sécurisés. Point de conformité avec les réglementations en matière de sécurité.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Rapport détaillé des mises à jour réalisées Plan de maintenance pour la gestion continue des serveurs.

Fiche-Action n°11_bis : Déployer systématiquement les mises à jour sur les serveurs du SI industriel

Description	Mesure visant au déploiement de solutions antivirus et anti-malware pour détecter et prévenir les menaces informatiques en temps réel.
Phases du projet	Préparation : Identification des serveurs industriels concernés. Analyse : Sélection des solutions adaptées en fonction des besoins de l'entreprise. Mise en œuvre : Installation, configuration, et lancement d'un premier scan complet des serveurs industriels. Restitution : Rapport des configurations et recommandations pour la maintenance.
Méthodologie	Utilisation de solutions reconnues sur le marché pour leur protection efficace en temps réel. Déploiement initial en environnement pilote avant la généralisation. Assistance technique pour les mises à jour et la maintenance.
Prérequis pour l'entreprise	Inventaire des équipements industriels à protéger. Accès aux configurations réseaux et serveurs concernés.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Protection proactive contre les menaces informatiques. Réduction des risques d'infections et des interruptions de service. Point de conformité avec les réglementations en matière de sécurité.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Rapport détaillé des mises à jour réalisées Plan de maintenance pour la gestion continue des serveurs.

Fiche-Action n°12 : Fermer tous les flux et les ports non strictement nécessaires

Description	L'objectif de cette mesure est de réduire drastiquement la surface d'attaque en fermant tous les ports et flux réseaux qui ne sont pas strictement nécessaires au bon fonctionnement de l'infrastructure.
Phases du projet	Préparation : Identification des ports et des flux actifs, recenser les services et applications en fonctionnement sur le réseau, vérifier les règles de filtrages sur les équipements réseau et firewall. Mise en œuvre : Désactiver les services inutilisés, restreindre les accès à certaines IP, bloquer les ports inutilisés. N'autoriser que les flux essentiels, isoler les services critiques (segmentation vLAN). Restitution : Rapport des nouvelles configurations.
Méthodologie	L'approche s'appuie sur les standards de sécurité. Déploiement progressif avec test à chaque étape. Si possible, automatisation des contrôles (SIEM, IDS/IPS, ScanVuln.) Transfert de compétences pour les mises à jour et la maintenance.
Prérequis pour l'entreprise	Inventaire des besoins métiers et des services légitimes. Accès aux firewall, routeurs et switchs. Validation des responsables métiers et IT.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 7	4 à 10
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction de la surface d'exposition et protection contre les attaques du réseau. Amélioration des performances réseau. Conformité aux standards de cybersécurité (ANSSI, ISO, NIST…). Renforcement de la sécurité sans impact sur le quotidien.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Politique de gestion des flux. Journal des modifications (à maintenir à jour)

Fiche-Action n°13 : Activer et conserver l'historique de l'ensemble des flux bloqués et des flux entrants et sortants identifiés par le pare-feu

Description	L'objectif de cette mesure est d'activer la journalisation des flux réseau (bloqués, entrants et sortants), de conserver ces logs de manière sécurisée et de les exploiter pour améliorer la cybersécurité de l'entreprise.
Phases du projet	Préparation : Vérification de la configuration de journalisation des firewall périmétriques et locaux. Vérification de la capacité de stockage et de rétention des logs. Mise en œuvre : Activation des logs pour les connexions bloquées entrantes et sortantes, configurer le niveau de détail des logs et la période de rétention (6 mois selon RGPD / 1 an selon ANSSI). Sécuriser les logs en suppression/modification. Centraliser les logs sur un serveur dédié (si possible vers un SIEM). Restitution : Rapport des configurations et recommandations pour la maintenance.
Méthodologie	Approche s'appuyant sur les standards de cybersécurité (ISO, ANSSI, NIST…) Déploiement initial en environnement pilote avant la généralisation. Transfert de compétences pour le suivi et la maintenance.
Prérequis pour l'entreprise	Accès aux firewalls périmétriques et locaux. Mise à disposition d'un serveur dédié et de capacité suffisante. Désignation d'un responsable IT pour l'exploitation et l'analyse.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 7	4 à 10
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Amélioration drastique de la détection des attaques. Traçabilité pour les missions de forensiques. Protection contre la suppression malveillante des traces. Renforcement de la conformité réglementaire (RGPD, ANSSI, ISO).
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Journalisation active et configurée sur l'ensemble des firewalls. Centralisation et sécurisation des logs opérationnelle. Exemple de tableau de suivi des incidents détectés à partir des logs.

Fiche-Action n°14 : Déployer un pare-feu physique pour protéger l'interconnexion du SI à Internet

Description	Mesure ayant pour but de déployer un firewall physique de type UTM (Unified Threat Management), une solution de sécurité tout-en-un qui permet de protéger le réseau d'une entreprise en filtrant le trafic entrant et sortant. Contrairement à un simple pare-feu logiciel, une UTM intègre plusieurs fonctionnalités avancées (filtrages des connexions, détections des intrusions, contrôle des applications, VPN, …).
Phases du projet	Préparation : analyse des besoins et de l'architecture réseau. Configuration : paramétrage du firewall et configuration d'un maximum de 100 règles de sécurité. Activation : déploiement des fonctions UTM, activation des logs Test : validation du fonctionnement.
Méthodologie	Configuration suivant les bonnes pratiques de sécurité. Cloisonnement des réseaux bureautique et industriel. Transfert de compétences aux utilisateurs et responsables IT pour une exploitation optimale de la solution. L'approche privilégie l'équilibre entre protection et usage.
Prérequis pour l'entreprise	Firewall compatible UTM, cartographie des réseaux et des flux entrants/sortants, désignation d'un responsable pour la gestion du firewall au quotidien.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	L'UTM offre une protection multicouche contre les cybermenaces tout en centralisant la gestion de la sécurité. Cette solution apporte une visibilité accrue sur les menaces et simplifie l'administration de la sécurité.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Firewall UTM configuré et opérationnel. Documentation de la configuration et des règles de filtrage implémentées. Procédures d'administration, et guide utilisateur.

Fiche-Action n°14_bis : Déployer un pare-feu physique pour cloisonner les réseaux industriels et bureautiques

Description	Mesure ayant pour but de déployer un firewall physique de type UTM (Unified Threat Management), une solution de sécurité tout-en-un qui permet de cloisonner l'interconnexion du réseau d'une entreprise au réseau industriel en filtrant le trafic entrant et sortant.
Phases du projet	Préparation : analyse des besoins et de l'architecture réseau. Configuration : paramétrage du firewall et configuration d'un maximum de 100 règles de sécurité. Activation : déploiement des fonctions UTM, activation des logs Test : validation du fonctionnement.
Méthodologie	Configuration suivant les bonnes pratiques de sécurité. Cloisonnement des réseaux bureautiques et industriels selon les standards de sécurité actuels. Transfert de compétences aux responsables IT pour une exploitation optimale de la solution. L'approche privilégie l'équilibre entre protection et usage.
Prérequis pour l'entreprise	Firewall compatible UTM, cartographie des réseaux et des flux entrants/sortants, désignation d'un responsable pour la gestion du firewall au quotidien.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	L'UTM offre une protection multicouche contre les cybermenaces tout en centralisant la gestion de la sécurité. Cette solution apporte une visibilité accrue sur les menaces et simplifie l'administration de la sécurité.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Firewall UTM configuré et opérationnel. Documentation de la configuration et des règles de filtrage implémentées. Procédures d'administration, et guide utilisateur.

Fiche-Action n°15 : Mettre en œuvre une solution d'anti-spam et d'anti-hameçonnage

Description	Mesure en faveur de la mise en œuvre d'une solution de protection de la messagerie pour détecter et bloquer les menaces ciblées (spams, phishing, ransomware, liens frauduleux, pièces jointes suspectes, etc.).
Phases du projet	Préparation : Identification des besoins en protection de la messagerie et choix de la solution adaptée. Analyse : Prise en compte des paramètres de protection et de compatibilité avec les systèmes existants. Mise en œuvre : Installation, configuration et tests de la solution. Restitution : Présentation des résultats et recommandations.
Méthodologie	Analyse des menaces récurrentes et des emails indésirables reçus. Déploiement progressif en mode POC afin de valider les performances et l'efficacité de la solution. Transfert de compétences aux utilisateurs et responsables IT pour une exploitation optimale de la solution.
Prérequis pour l'entreprise	Accès aux systèmes de messagerie existants. Liste des utilisateurs et des domaines à protéger. Définition d'un responsable pour l'administration de la solution.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 3	4 à 5	4 à 5
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction des risques de phishing et d'attaques ciblées. Amélioration de la sécurité de la messagerie électronique en réduisant le risque d'erreurs humaines. Gain de productivité en limitant le temps perdu à gérer les spams. Gain sur capacités de stockage en bloquant les mails indésirables.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Solution antispam/anti-phishing opérationnelle. Politique de sécurité de la messagerie. Plan de déploiement.

Fiche-Action n°16 : Recourir à un chiffrement robuste du réseau Wi-Fi

Description	Mesure visant à la mise en œuvre d'un chiffrement robuste pour les connexions au réseau Wi-Fi interne et assurer la gestion des invités.
Phases du projet	Préparation : Identification des réseaux publiés/accessibles et vérification de leurs paramètres de sécurité actuels. Analyse : Vérification de la compatibilité des postes et terminaux. Mise en œuvre : Désactivation des protocoles obsolètes, désactivation du SSID Broadcast, activation du WPA-2 ou WPA3, définition de mots de passe robustes, activation du filtrage MAC, mise en place d'un réseau « Invités » isolé (avec journaux) Restitution : Rapport des configurations et guide d'utilisation.
Méthodologie	Diagnostic initial des réseaux existants Déploiement progressif en mode POC. Tests initiaux pour vérifier la compatibilité. Transfert de compétences aux utilisateurs et responsables IT.
Prérequis pour l'entreprise	Liste des équipements Wi-Fi disponibles. Liste des équipements (PC, smartphones, tablettes…) qui sont autorisés à se connecter. Accès aux équipements réseau (box, routeurs, bornes…)

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 3	4 à 5	4 à 5
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Sécurisation des accès WiFi Réduction des risques liés aux accès non autorisés. Isolation et limitation des connexions des invités.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Réseau WiFi plus robuste et cloisonné suivant les utilisateurs. Politique de gestion des réseaux sans fil.

Fiche-Action n°17 : Protéger l'accès à l'espace de stockage des serveurs et des équipements réseau par une porte pouvant être fermée à clef

Description	Mesure visant à garantir un accès restreint et sécurisé aux infrastructures critiques en les installant dans une salle ou une armoire fermée à clé, accessible uniquement aux personnes autorisées.
Phases du projet	Préparation : Identification des équipements sensibles (serveurs baies de stockage, routeurs switchs, firewalls…), et inventaire des personnes autorisées à accéder aux équipements. Analyse : Sélection de la solution adaptée en fonction des besoins de l'entreprise (salle dédiée, baie informatique, local technique). Si possible, prévoir un contrôle d'accès technique (badges RFID/NFC, tokens, code d'accès, contrôle biométrique…). Et si nécessaire prévoir la détection d'intrusion et une alarme. Réflexion sur les restrictions d'accès hors plage horaire. Mise en œuvre : Installation d'un verrou de sécurité (et d'une alarme) ou d'une solution technologique. Restitution : Rapport des autorisations/restrictions et recommandations pour la maintenance.
Méthodologie	Approche s'appuyant sur les standards de sécurité (ANSSI, ISO…) Transfert de compétences pour la maintenance.
Prérequis pour l'entreprise	Liste des personnes autorisées (et des plages horaires). Identification des locaux dédiés aux équipements. Budget pour la mise en place de contrôle d'accès électronique.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	1 à 4	2 à 6	2 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction des risques de sabotage ou de vol de matériel. Conformité aux bonnes pratiques de cybersécurité. Maitrise et traçabilité des accès aux équipements critiques.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Salle informatique avec accès protégé et journalisé. Registre des accès et des personnes autorisées. Procédure de gestion des accès.

4. Sécuriser les accès

La sécurité des accès consiste à contrôler et protéger l'authentification et les autorisations des utilisateurs qui se connectent aux ressources informatiques de l'entreprise (postes de travail, serveurs, applications cloud, VPN, etc.).

Une mauvaise gestion des accès peut permettre à des attaquants d'exploiter des identifiants volés, des mots de passe faibles ou des accès mal configurés pour infiltrer le système d'information, voler des données ou exécuter des actions malveillantes.

Ce thème couvre plusieurs aspects essentiels :

- L'authentification sécurisée (mots de passe forts, authentification multi-facteurs...).
- La gestion des comptes et des privilèges
- La surveillance et la détection des accès suspects.

Un accès non-maîtrisé au système d'information représente un risque majeur de cyberattaques, notamment :

- Le vol de données sensibles (comptes clients, données bancaires, fichiers confidentiels).
- La prise de contrôle des systèmes via des comptes administrateurs mal protégés.
- La propagation de logiciels malveillants exploitant des accès non sécurisés.

En sécurisant les accès, l'entreprise réduit considérablement le risque de compromission et renforce la traçabilité des connexions.

En résumé, la sécurisation des accès et des droits est un élément fondamental de la cybersécurité. En mettant en place des contrôles stricts et des bonnes pratiques d'authentification, même une petite entreprise peut significativement réduire son exposition aux menaces.

Fiche-Action n°18 : Limiter drastiquement le nombre d'utilisateurs disposant du privilège d'administration local sur leur machine.

Description	La mesure consiste à mettre en place des comptes d'administration dédiés, distincts des comptes utilisateurs standards. Dans le même temps de limiter et (au besoin) même supprimer, les droits d'administration locale sur les postes de travail. *Rappel : Les comptes administrateurs permettent d'effectuer des actions critiques sur le système d'information (installation de logiciels, modification des paramètres système, gestion des utilisateurs).*
Phases du projet	Préparation : Identification des comptes administrateurs existants, qu'ils soient sur le réseau ou locaux. Analyse : Si nécessaire, mener une réflexion autour d'une solution alternative comme LAPS ou PAM. Mise en œuvre : Création de comptes dédiés et suppression des comptes locaux d'administration. Restitution : Tests et remise des supports pédagogiques.
Méthodologie	Implémentation du « principe du moindre privilège » (seuls les comptes dédiés et autorisés ont des droits d'administration). Déploiement progressif en monde POC. Contrôle et validation du dispositif.
Prérequis pour l'entreprise	Inventaire des comptes administrateurs et les accès associés. Accès aux configurations des systèmes cibles. Implication des équipes IT pour la mise en œuvre. Accès aux outils de gestion centralisée (si existants).

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 8
TJM préconisé	Profil : Technicien/Admin → 400€/j			

Valeur ajoutée	Réduction des risques de compromission. Renforcement de la sécurité des postes et des serveurs. Conformité aux bonnes pratiques ANSSI. Protection accrue contre les ransomwares.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Liste des nouveaux comptes d'administration dédiés. Liste des comptes d'administration locaux supprimés. Politique de gestion des comptes administrateurs

Fiche-Action n°19 : Utiliser des comptes d'administration dédiées à cet usage, les administrateurs disposant en parallèle d'un compte utilisateur. Utiliser également des comptes d'administration distincts dédiés à l'administration de l'AD/Samba-AD et à la solution de sauvegarde.

Description	La mesure consiste à mettre en place des comptes d'administration dédiés, distincts des comptes utilisateurs standards. Dans le même temps de limiter et (au besoin) même supprimer, les droits d'administration locale sur les postes de travail. *Rappel : Les comptes administrateurs permettent d'effectuer des actions critiques sur le système d'information (installation de logiciels, modification des paramètres système, gestion des utilisateurs).*
Phases du projet	Préparation : Identification des comptes administrateurs existants, qu'ils soient sur le réseau ou locaux. Analyse : Si nécessaire, mener une réflexion autour d'une solution alternative comme LAPS ou PAM. Mise en œuvre : Création de comptes dédiés et suppression des comptes locaux d'administration. Restitution : Tests et remise des supports pédagogiques.
Méthodologie	Implémentation du « principe du moindre privilège » (seuls les comptes dédiés et autorisés ont des droits d'administration). Déploiement progressif en monde POC. Contrôle et validation.
Prérequis pour l'entreprise	Inventaire des comptes administrateurs et les accès associés. Accès aux configurations des systèmes cibles. Implication des équipes IT pour la mise en œuvre. Accès aux outils de gestion centralisée (si existants).

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Technicien/Admin → 400€/j			

Valeur ajoutée	Réduction des risques de compromission et renforcement de la sécurité des postes et des serveurs. Conformité aux bonnes pratiques
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Liste des nouveaux comptes d'administration dédiés. Liste des comptes d'administration locaux supprimés. Politique de gestion des comptes administrateurs

Fiche-Action n°20 : Mettre en place selon les possibilités, un mécanisme d'authentification multifacteur pour accéder aux comptes d'administration à hauts privilèges ainsi que des contraintes renforcées de robustesse et de longueur de mots de passe (15 car. minimum)

Description	Mesure consistant à la mise en place d'une authentification multifacteurs (MFA) pour protéger les accès aux systèmes et données critiques de l'entreprise.
Phases du projet	Préparation : Identification des comptes critiques concernés. Analyse : Choix d'une solution MFA adaptée (applications mobiles, clés physiques, SMS, mail, etc.). Mise en œuvre : Déploiement, configuration des systèmes, et formation des utilisateurs. Restitution : Tests et remise des supports pédagogiques.
Méthodologie	Intégration de la solution MFA avec les systèmes existants. Déploiement progressif en mode POC. Tests pilotes pour garantir la compatibilité et l'adoption. Transfert de compétences aux utilisateurs et responsables IT.
Prérequis pour l'entreprise	Inventaire des systèmes et utilisateurs concernés. Accès aux configurations des systèmes cibles. Accès aux outils de gestion centralisée (si existants). Communication interne pour informer et accompagner les utilisateurs.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 8	4 à 8
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction des risques de compromission. Amélioration significative de la sécurité des accès critiques. Conformité aux bonnes pratiques et alignement avec le RGPD. Protection accrue contre les attaques par hameçonnage.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. MFA activée sur les comptes critiques. Politique de gestion des accès. Supports pédagogiques pour les utilisateurs.

Fiche-Action n°21 : Mettre en place pour tous les accès distants des mécanismes d'authentification multifacteur à minima, avec restriction via adresses IP (ex : localisation, pays, plages horaires)

Description	Mesure consistant à la mise en place d'une authentification multifacteurs (MFA) pour protéger les accès distants aux systèmes et données critiques de l'entreprise.
Phases du projet	Préparation : Identification des utilisateurs distants et des comptes critiques concernés. Analyse : Choix d'une solution MFA adaptée (applications mobiles, clés physiques, SMS, mail, etc.). Mise en œuvre : Déploiement, configuration des systèmes, et formation des utilisateurs. Restitution : Tests et remise des supports pédagogiques.
Méthodologie	Intégration de la solution MFA avec les systèmes existants. Déploiement progressif en mode POC. Tests pilotes pour garantir la compatibilité et l'adoption. Transfert de compétences aux utilisateurs et responsables IT.
Prérequis pour l'entreprise	Inventaire des systèmes et utilisateurs concernés. Accès aux configurations des systèmes cibles. Accès aux outils de gestion centralisée (si existants). Communication interne pour informer et accompagner les utilisateurs.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 8	4 à 8
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction des risques de compromission. Amélioration significative de la sécurité des accès distants. Conformité aux bonnes pratiques et alignement avec le RGPD. Protection accrue contre les attaques par hameçonnage.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. MFA activée sur les comptes d'utilisateurs distants. Politique de gestion des accès distants. Supports pédagogiques pour les utilisateurs.

Fiche-Action n°21_bis : Mettre en place pour tous les accès distants du SI industriel des mécanismes d'authentification multifacteur à minima, avec restriction via adresses IP (localisation, plages horaires…)

Description	Mesure consistant à la mise en place d'une authentification multifacteurs (MFA) pour protéger les accès aux systèmes et données du SI industriel.
Phases du projet	Préparation : Identification des utilisateurs nécessitant un accès aux postes du SI industriel. Analyse : Choix d'une solution MFA adaptée (applications mobiles, clés physiques, SMS, mail, etc.). Mise en œuvre : Déploiement, configuration des systèmes, et formation des utilisateurs. Restitution : Tests et remise des supports pédagogiques.
Méthodologie	Intégration de la solution MFA avec les systèmes industriels existants. Déploiement progressif en mode POC. Tests pilotes pour garantir la compatibilité et l'adoption. Transfert de compétences aux utilisateurs et responsables IT.
Prérequis pour l'entreprise	Inventaire des systèmes industriels et utilisateurs concernés. Accès aux configurations des systèmes cibles. Accès aux outils de gestion centralisée (si existants). Communication interne pour informer et accompagner les utilisateurs.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 8	4 à 8
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction des risques de compromission. Amélioration significative de la sécurité des accès au SI industriel. Conformité aux bonnes pratiques et alignement avec les standards. Protection accrue contre les attaques réseau.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. MFA activée sur les comptes d'utilisateurs impliqués sur le SI industriel Politique de gestion des accès industriel. Supports pédagogiques pour les utilisateurs.

Fiche-Action n°22 : Restreindre l'accès aux données à protéger en priorité aux seules personnes autorisées à y accéder (ex : un tableau répertoriant les utilisateurs légitimes par systèmes/applications à protéger en priorité)

Description	L'objectif de cette mesure est de répertorier, restreindre et surveiller l'accès aux données critiques. Veillant ainsi à ce qu'un utilisateur n'accède qu'aux informations strictement nécessaires à son travail
Phases du projet	Préparation : Identification des informations sensibles et des systèmes ou applications critiques hébergeant ces données. Mise en œuvre : Création d'un tableau de gestion des accès, application d'un contrôle basé sur les rôles, implémentation d'un processus de validation et de revue des accès.
Méthodologie	Implémentation du « principe du moindre privilège » (seuls les comptes dédiés et autorisés ont des droits d'administration). Déploiement progressif en monde POC. Contrôle et validation du dispositif.
Prérequis pour l'entreprise	Inventaire des systèmes, applications et utilisateurs concernés. Désignation d'un responsable pour la gestion des accès. Accès aux configurations des systèmes cibles. Accès aux outils de gestion centralisée (si existants). Communication interne pour informer et accompagner les utilisateurs.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 8	6 à 10
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction des risques de fuites ou de compromission. Protection contre les menaces internes. Amélioration significative de la sécurité et de la traçabilité. Conformité aux bonnes pratiques ANSSI et alignement avec le RGPD. Simplification de la gestion des accès sensibles.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Tableau de gestion des accès sensibles. Processus de revue/attribution régulière des accès.

Fiche-Action n°23 : Fixer des contraintes de longueur et de complexité des mots de passe exigeant à minima 12 caractères incluant minuscules, majuscules, chiffres et caractères spéciaux, 16 caractères pour les utilisateurs détenant les droits d'administration local de leur poste de travail.

Description	Mesure qui vise à définir et appliquer une politique de gestion des mots de passe robustes afin de réduire drastiquement les risques de compromission et d'assurer une meilleure protection des accès.
Phases du projet	Préparation : communication interne pour informer et accompagner les utilisateurs. Analyse : Si besoin mettre en place des mesures complémentaires (gestionnaire/coffre-fort numérique/MFA) Mise en œuvre : Définition d'une politique de création de mots de passe, application à l'ensemble du SI.
Méthodologie	Analyse des pratiques actuelles. Définition et validation de la politique. Déploiement progressif (si nécessaire).
Prérequis pour l'entreprise	Accès aux outils de gestion des comptes. Identification des services nécessitant une maj régulière. Communication ou sensibilisation auprès des utilisateurs.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	3 à 5	3 à 5
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction significative des risques de compromission. Renforcement de la protection des accès. Conformité avec les bonnes pratiques ANSSI.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Politique générale de gestion des mots de passe.

Fiche-Action n°24 : Réaliser annuellement une revue des accès utilisateurs en les comparant avec les informations détenues par le service RH. Les mots de passes des comptes partagés concernés sont renouvelés à chaque départ.

Description	Mesure consistant à la mise en place d'un processus de revue/attribution annuelle des accès et des privilèges permettant de vérifier qui a accès à quoi, d'identifier et supprimer les comptes inutiles, et de réduire les risques d'intrusion en s'assurant que seuls les utilisateurs autorisés ont des accès au SI.
Phases du projet	Préparation : Inventaire des accès et droits existants, ainsi que des utilisateurs concernés. Analyse : Identification des comptes inactifs ou orphelins, détection des droits « excessifs ». Mise en œuvre : Suppression, correction ou optimisation des comptes, validation collégiale des modifications. Restitution : Rédaction d'un processus de revue régulière.
Méthodologie	Nomination d'un comité de revue. Analyse préalable des accès et identification des écarts. Remédiation progressive et vérification. Automatisation du suivi (si possible), ou comitologie.
Prérequis pour l'entreprise	Accès aux annuaires d'utilisateurs. Identification des systèmes et applications critiques. Implication des responsables métiers, IT et de la direction.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	5 à 8	5 à 8
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Meilleure gestion des identités. Réduction du risque d'accès non-autorisés. Sécurisation des accès sensibles. Point de conformité aux bonnes pratiques ANSSI et RGPD.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de mission. Tableau de suivis des accès et privilèges. Processus de revue récurrente.

Fiche-Action n°24_bis : Réaliser tous les 6 mois une revue des accès utilisateurs en les comparant avec les informations détenues par le service RH. Les mots de passes des comptes partagés concernés sont renouvelés à chaque départ.

Description	Mesure consistant à la mise en place d'un processus de revue/attribution semestrielle des accès et des privilèges permettant de vérifier qui a accès à quoi, d'identifier et supprimer les comptes inutiles, et de réduire les risques d'intrusion en s'assurant que seuls les utilisateurs autorisés ont des accès au SI.
Phases du projet	Préparation : Inventaire des accès et droits existants, ainsi que des utilisateurs concernés. Analyse : Identification des comptes inactifs ou orphelins, détection des droits « excessifs ». Mise en œuvre : Suppression, correction ou optimisation des comptes, validation collégiale des modifications. Restitution : Rédaction d'un processus de revue régulière.
Méthodologie	Nomination d'un comité de revue. Analyse préalable des accès et identification des écarts. Remédiation progressive et vérification. Automatisation du suivi (si possible), ou comitologie.
Prérequis pour l'entreprise	Accès aux annuaires d'utilisateurs. Identification des systèmes et applications critiques. Implication des responsables métiers, IT et de la direction.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	5 à 8	5 à 8
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Meilleure gestion des identités. Réduction du risque d'accès non-autorisés. Sécurisation des accès sensibles. Point de conformité aux bonnes pratiques ANSSI et RGPD.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de mission. Tableau de suivis des accès et privilèges. Processus de revue récurrente.

Fiche-Action n°25 : Mettre en place selon les possibilités, un mécanisme d'authentification multifacteur pour accéder aux données jugées les plus sensibles et/ou des contraintes renforcées de robustesse et de longueur de mots de passe (16 caractères minimum)

Description	Mesure consistant à la mise en place d'une authentification multifacteurs (MFA) pour protéger les accès distants aux données jugées sensibles ou critiques pour l'entreprise.
Phases du projet	Préparation : Identification des données sensibles et/ou critiques. Analyse : Choix d'une solution MFA adaptée (applications mobiles, clés physiques, SMS, mail, etc.). Mise en œuvre : Déploiement, configuration des systèmes, et formation des utilisateurs. Restitution : Tests et remise des supports pédagogiques.
Méthodologie	Intégration de la solution MFA avec les systèmes existants. Déploiement progressif en mode POC. Tests pilotes pour garantir la compatibilité et l'adoption. Transfert de compétences aux utilisateurs et responsables IT.
Prérequis pour l'entreprise	Inventaire des données sensibles/critiques et des utilisateurs autorisés Accès aux configurations des systèmes cibles hébergeant ces données. Communication interne pour informer et accompagner les utilisateurs.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 8	4 à 8
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réduction des risques de compromission. Amélioration significative de la sécurité des données sensibles/critiques Conformité aux bonnes pratiques et alignement avec le RGPD.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. MFA activée sur les accès aux données sensibles et/ou critiques. Politique de gestion des accès sensibles et/ou critiques. Supports pédagogiques pour les utilisateurs.

Fiche-Action n°26 : Mettre en œuvre un outil de gestion des politiques de sécurité centralisé (ex : AD, Samba-AD) et en évaluer/améliorer son niveau de sécurité annuellement, idéalement au travers d'un accompagnement extérieur.

Description	Mesure ayant pour objectif d'implémenter un annuaire LDAP (Lightweight Directory Access Protocol) permettant de centraliser la gestion des identités et des accès, de faciliter l'authentification des utilisateurs et d'appliquer des politiques de sécurité uniformes sur l'ensemble du SI.
Phases du projet	Préparation : Identification de l'ensemble des utilisateurs. Installation : déploiement de l'annuaire et définition initiale de la structure de l'annuaire, intégration des services et applications. Configuration : paramétrage des politiques, configuration des journaux, tests de validation. Formation : transfert de compétences aux administrateurs.
Méthodologie	Mise en œuvre progressive avec validation à chaque étape du déploiement. L'approche privilégie les solutions éprouvées (ex : Active Directory) et compatibles avec l'infrastructure existante. Configuration basée sur les bonnes pratiques ANSSI.
Prérequis pour l'entreprise	Liste des systèmes et applications à intégrer dans le LDAP. Définir un serveur dédié à l'hébergement du LDAP. Implication des équipes IT pour la configuration et la maintenance.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 5	4 à 8	4 à 10
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	La centralisation et simplification de la gestion des comptes. Facilité d'administration des comptes et des politiques de sécurité. Renforcement de la sécurité et de la traçabilité. Réduction des erreurs humaines. Conformité réglementaire.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Solution de gestion centralisée déployée et opérationnelle. Liste des systèmes et applications intégrés à l'annuaire. Guide d'administration et procédures de maintenance.

5. Réagir à un incident ou une attaque

Aucune entreprise, quelle que soit sa taille, n'est à l'abri d'un incident de cybersécurité. Attaque par ransomware, compromission de compte, fuite de données, sabotage interne… les menaces sont multiples et évoluent constamment.

Face à une attaque, la capacité de réaction est un élément clé pour limiter les dégâts, restaurer l'activité rapidement et éviter une récidive. Une entreprise qui anticipe et prépare sa réponse aux incidents réduit considérablement ses pertes financières et réputationnelles.

Une mauvaise gestion d'un incident peut entraîner :

- Une interruption prolongée des services impactant l'activité et la productivité.
- Une perte ou un vol de données sensibles pouvant nuire aux clients et partenaires.
- Des sanctions juridiques et financières en cas de non-respect des réglementations (RGPD, NIS2…).
- Un impact réputationnel fort, diminuant la confiance des clients et collaborateurs.

En revanche, une réaction rapide et structurée permet de reprendre le contrôle et d'adopter les bonnes mesures pour éviter qu'un incident ne se reproduise.

En résumé, réagir efficacement à un incident ne s'improvise pas. Une préparation en amont, une organisation claire et des procédures bien définies permettent de gérer un incident ou une cyberattaque avec sang-froid et efficacité.

Fiche-Action n°27 : Réaliser des sauvegardes régulières autant que de besoin et dont le rythme est jugé acceptable par le CODIR.

Description	Mesure visant à l'installation et la configuration d'une solution de sauvegarde locale incluant le matériel et les logiciels nécessaires. Ce service assure la protection des données critiques de l'entreprise sur site.
Phases du projet	Préparation : analyse des besoins et sélection de la solution. Installation : mise en place du matériel et des logiciels. Configuration : paramétrage des sauvegardes et tests initiaux. Formation : transfert de compétences aux administrateurs.
Méthodologie	Déploiement structuré utilisant des solutions éprouvées du marché. Les configurations suivent les bonnes pratiques de sécurité et de performance.
Prérequis pour l'entreprise	Infrastructure technique adaptée et espace de stockage disponible.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Le système de sauvegarde local permet une protection efficace des données avec des temps de restauration optimisés grâce à la proximité des sauvegardes. Cette solution offre une autonomie complète dans la gestion des sauvegardes tout en garantissant la confidentialité des données.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Solution de sauvegarde locale opérationnelle. Documentation technique, procédures d'exploitation. Journal des tests, support de formation.

Fiche-Action n°28 : Procéder régulièrement à des tests de restauration

Description	Mesure visant à réaliser de tests complets de restauration pour valider l'efficacité des sauvegardes et la capacité de l'entreprise à récupérer ses données. Ces tests permettent de vérifier les procédures et les temps de reprise.
Phases du projet	Préparation : définition des scénarios et préparation des environnements. Exécution : réalisation des tests de restauration. Vérification : contrôle des données restaurées. Restitution : analyse des résultats et recommandations.
Méthodologie	Tests structurés couvrant différents scénarios de restauration. Les vérifications incluent l'intégrité des données et les performances.
Prérequis pour l'entreprise	Système de sauvegarde opérationnel et environnement de test disponible.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Technicien → 400€/j			

Valeur ajoutée	Les tests de restauration valident concrètement la capacité de l'entreprise à récupérer ses données en cas d'incident. Cette démarche permet d'identifier les améliorations nécessaires et de former les équipes aux procédures de restauration.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Rapport des tests effectués. Métriques de restauration. Recommandations d'amélioration. Journal des anomalies.

Fiche-Action n°29 : Disposer d'une sauvegarde des données critiques stockées dans un environnement sécurisé, isolé de l'environnement bureautique et d'internet, en complément des sauvegardes régulièrement réalisées et stockées sur le réseau

Description	Mesure visant à l'installation et la configuration d'une solution de sauvegarde amovible, transportable et stockable, ou cloud. Ce service assure la protection des données critiques de l'entreprise hors-site.
Phases du projet	Préparation : analyse des besoins et sélection de la solution. Installation : mise en place du matériel et des logiciels. Configuration : paramétrage des sauvegardes et tests initiaux. Formation : transfert de compétences aux administrateurs.
Méthodologie	Déploiement structuré utilisant des solutions éprouvées du marché. Les configurations suivent les bonnes pratiques de sécurité et de performance.
Prérequis pour l'entreprise	Disposer d'une sauvegarde locale à dupliquer sur un support amovible ou dans le cloud. Disposer d'un espace de stockage externalisable ou cloud.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 4	4 à 6	4 à 6
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Le système de sauvegarde externalisée permet une protection efficace des données avec un risque moindre de compromission (ransomware, vol, incendie, inondation, ...). Cette solution offre un niveau supplémentaire de résilience.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Solution de sauvegarde externalisable opérationnelle. Documentation technique, procédures d'exploitation. Journal des tests, support de formation.

Fiche-Action n°30 : Lister les personnes à contacter en cas d'incident de sécurité informatique (cellule de crise)

Description	Mesure visant à définir une liste des personnes à contacter en cas d'incident, en précisant leurs rôles, responsabilités et moyens de communication. Cette « cellule de crise » permet d'avoir une chaîne de commandement efficace et d'assurer une coordination rapide des actions de réponse.
Phases du projet	Préparation : identification des rôles clés dans la gestion de crise (direction, référent cyber, conformité, communication, prestataires…). Mise en œuvre : élaboration de la liste (noms, fonctions, rôles, disponibilité…). Définition d'un protocole de communication (interne, externe, institutionnel). Définition des premières actions urgentes à mener. Livraison : Mise à disposition du document et stockage sécurisé.
Méthodologie	Recensement et structuration de la liste, définition d'un protocole clair basé sur les bonnes pratiques de la réponse à incident cyber.
Prérequis pour l'entreprise	Identification des parties prenantes, mais aussi de leurs rôles et responsabilités.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 3	3 à 5	3 à 5
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Réactivité accrue en cas d'incident. Coordination plus efficaces moyens et des personnes. Réduction des impacts d'une cyberattaque. Sérénité et anticipation face à une crise cyber.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Liste des contacts de la cellule de crise. Procédures d'alerte et d'escalade.

Fiche-Action n°31 : Réaliser une veille trimestrielle sur internet (ex : veille des avis et alertes publiés sur le site du CERT-FR)

Description	Mesure ayant pour objectif la mise en place d'une veille cyber régulière permettant d'anticiper les risques, d'adopter les bonnes pratiques et de renforcer la sécurité des systèmes avant qu'une faille ne soit exploitée.
Phases du projet	Préparation : analyse des sources pertinentes (agences, fournisseurs, communautés, réseaux professionnels, légal, ...). Installation : mise en place d'outils de veille automatisés (flux RSS, alertes Google/X, outils spécialisés (Shodan, MISP, ...). Mise en œuvre : définition de mots clés, désignation d'un responsable de veille, choix des canaux de diffusion interne. Définition des actions en cas d'alerte critique.
Méthodologie	Sélection de sources vérifiées et fiables, automatisation, centralisation et intégration dans le plan d'actions cyber.
Prérequis pour l'entreprise	Choix d'un responsable, réflexion sur les sujets critiques à surveiller (vulnérabilités, métiers, réglementaire, ...)

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 3	3 à 4	3 à 4
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Anticipation des menaces et réactivité accrue. Montée en compétences des équipes et entretien de la culture IT. Amélioration de la résilience.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Installation d'outils spécialisés (si nécessaire). Liste des sources de veille et plan de diffusion interne. Procédure de réaction en cas d'alerte critique.

6. Sensibiliser les utilisateurs

Aucune entreprise, quelle que soit sa taille, n'est à l'abri d'un incident de cybersécurité. Attaque par ransomware, compromission de compte, fuite de données, sabotage interne… les menaces sont multiples et évoluent constamment.

Face à une attaque, la capacité de réaction est un élément clé pour limiter les dégâts, restaurer l'activité rapidement et éviter une récidive. Une entreprise qui anticipe et prépare sa réponse aux incidents réduit considérablement ses pertes financières et réputationnelles.

Une mauvaise gestion d'un incident peut entraîner :

- Une interruption prolongée des services impactant l'activité et la productivité.
- Une perte ou un vol de données sensibles pouvant nuire aux clients et partenaires.
- Des sanctions juridiques et financières en cas de non-respect des réglementations (RGPD, NIS2, DORA…).
- Un impact réputationnel fort, diminuant la confiance des clients et collaborateurs.

En revanche, une réaction rapide et structurée permet de reprendre le contrôle et d'adopter les bonnes mesures pour éviter qu'un incident ne se reproduise.

En résumé, réagir efficacement à un incident ne s'improvise pas. Une préparation en amont, une organisation claire et des procédures bien définies permettent de gérer un incident ou une cyberattaque avec sang-froid et efficacité.

Fiche-Action n°32 : Encourager régulièrement (2 fois/an à minima) la déclaration d'incident auprès de vos agents en rappelant les évènements « signaux faibles » devant être signalés ainsi que le contact à alerter. Formaliser et diffuser une fiche réflexe dédiée aux utilisateurs

Description	L'objectif de cette action est de renforcer la culture de la cybersécurité en permettant aux collaborateurs de signaler des évènements de tous types qui pourraient s'avérer être un incident ou signe d'une attaque.
Phases du projet	Préparation : identification des évènements à signaler (signaux faibles) comme un email suspect, ralentissement inhabituel du PC, pop-up étrange, appel téléphonique suspect, demande d'accès anormale… Mise en œuvre : Création d'une fiche réflexe et mise en place d'une procédure de déclaration (mail, contact IT, hotline, outil de ticketing…) Organisation de rappels semestriels pour les collaborateurs. Mise en place d'un processus de suivi des incidents signalés.
Méthodologie	Approche s'appuyant sur les standards (ANSSI, ISO, RGPD…) Diffusion en session de sensibilisation ou à l'arrivée de nouveaux collaborateurs, inscription dans la charte informatique.
Prérequis pour l'entreprise	Définition d'un point de contact référent pour les incidents. Implication des collaborateurs, des manageurs et des responsables IT.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 3	3 à 4	3 à 4
TJM préconisé	Profil : Ingénieur/Chef de projet → 600€/j			

Valeur ajoutée	Détection précoce de potentielles cyberattaques. Réduction des risques d'incidents majeurs. Amélioration de la culture cybersécurité et de la réactivité de l'IT. Point de conformité aux bonnes pratiques (ANSSI, ISO, RGPD).
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Fiche réflexe de déclaration d'incidents et le canal d'escalade dédié. Processus de gestion et de suivi des déclarations

Fiche-Action n°33 : Etablir une charte informatique répertoriant les moyens informatiques mis à disposition, clarifiant la gestion des terminaux personnels et rappelant à minima les exigences de cybersécurité liées à la gestion des comptes d'accès, des mots de passe, des données à protéger en priorités, de l'utilisation de la messagerie et des ressources cloud.

Description	Mesure qui vise à créer un document cadre pour l'utilisation des outils numériques, permettant de diffuser les règles de sécurité de l'entreprise, de protéger les actifs informatiques et de se conformer aux exigences du RGPD et des standards de sécurité ANSSI ou ISO.
Phases du projet	Préparation : Recensement des moyens informatiques, définition des règles d'usages (y compris pour les terminaux personnels), définition des règles de sécurité (mots de passe, MFA, accès sensibles, messagerie, stockage amovible, cloud...) Mise en œuvre : Rédaction, validation et diffusion de la charte. Mise en place d'un processus de revue périodique du document.
Méthodologie	Approche s'appuyant sur les standards (ANSSI, ISO, RGPD…). Rédaction collaborative et validation collégiale. Diffusion à l'arrivée de nouveaux collaborateurs, en session de sensibilisation ou encore affichage en zone commune.
Prérequis pour l'entreprise	Liste des outils et services numériques de l'entreprise. Exigences de sécurité (Politique de Sécurité du Système d'Information) Définition d'un référent IT ou Cybersécurité pour gérer et faire appliquer la charte dans l'entreprise.

Catégorie	TPE	PME	ETI	Org. publics
Public concerné	☑	☑	☑	☑
Durée estimée (j)	1 à 2	2 à 3	3 à 4	3 à 4
TJM préconisé	Profil : Consultant → 800€/j			

Valeur ajoutée	Réduction des risques liés à un mauvais usage des outils numériques. Conformité au RGDP et aux recommandations de l'ANSSI. Amélioration de la culture de cybersécurité. Sensibilisation et responsabilisation des collaborateurs.
Financement	Prise en charge par l'EDIH La Réunion : 65% du montant HT
Livrables	Rapport synthétique de la mission. Charte informatique et processus de mise à jour.