



La Continuité d'Activité et la Gestion de la Sécurité des Systèmes d'Information

SL

par Stéphane LARCHER

Table des matières

1. Introduction à la continuité d'activité
2. Le Système d'Information (SI)
3. Le Système de Gestion de la Sécurité de l'Information (ISMS)
4. Les incidents de sécurité
5. Cycle de vie d'un incident de sécurité
6. La réponse à incident

Introduction à la continuité d'activité

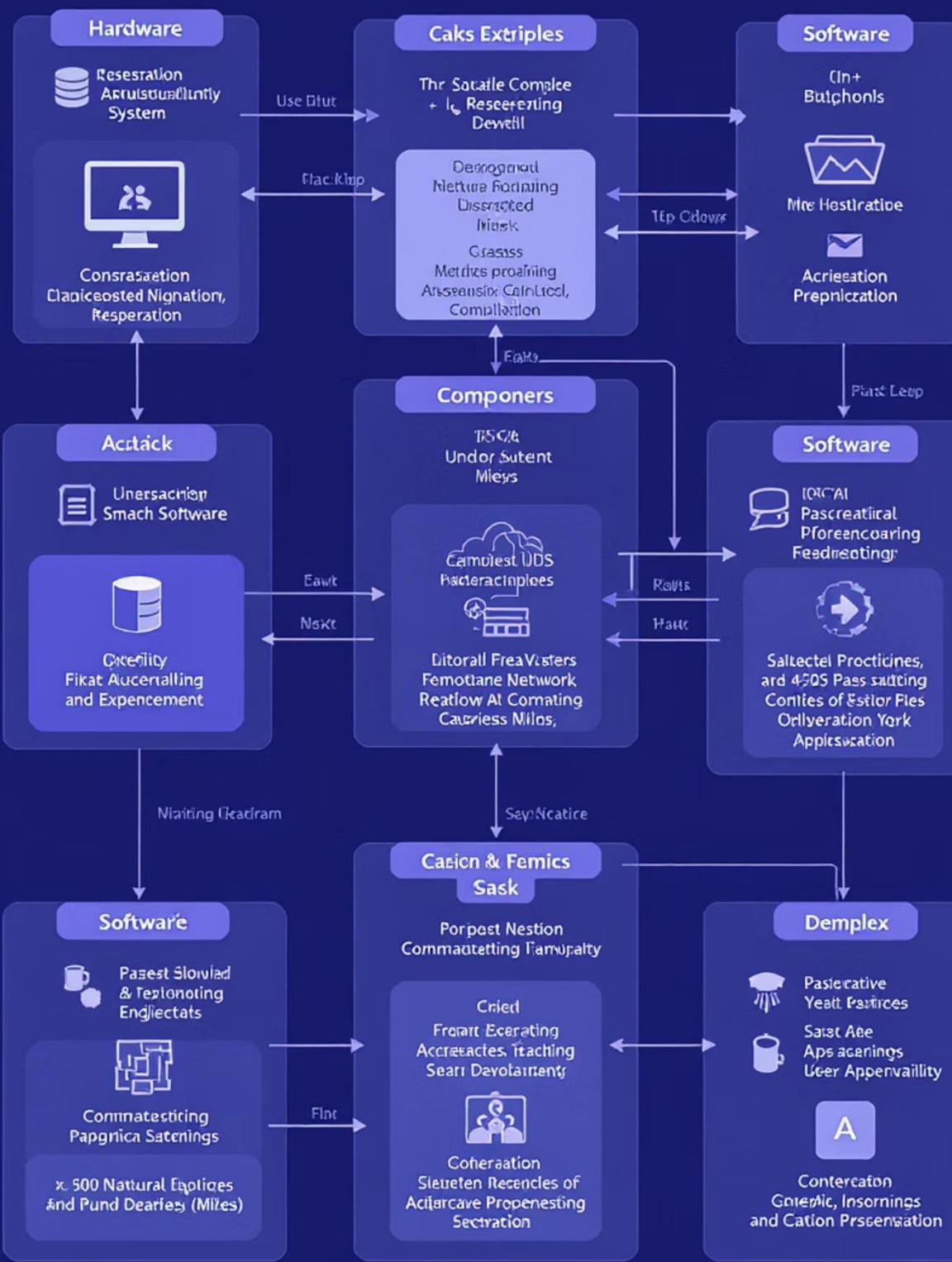
Définition

La **continuité d'activité** (Business Continuity) désigne l'ensemble des mesures visant à assurer le maintien ou le rétablissement rapide des activités critiques d'une organisation en cas d'incident majeur ou de crise.

Objectifs principaux

- Minimiser l'impact des interruptions sur les opérations
- Protéger les actifs informationnels critiques
- Garantir la disponibilité des services essentiels
- Maintenir la confiance des parties prenantes

Complex Information System Architecture



Le Système d'Information (SI)

Définition du SI

Le **Système d'Information** est l'ensemble organisé de ressources (matériels, logiciels, données, procédures, personnel) qui permet de collecter, traiter, stocker et distribuer l'information au sein d'une organisation.



Composantes spécifiques de sécurité



SSIV - Sécurité des Systèmes d'Information Vitaux

Définition : Protection des systèmes d'information dont l'indisponibilité ou la destruction aurait un impact majeur sur :

- La santé ou la sécurité de la population
- Le potentiel économique ou scientifique du pays
- La sécurité nationale



SSI - Sécurité des Systèmes d'Information

Définition : Ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires pour garantir la sécurité des systèmes d'information.

Les trois piliers de la SSI



Ces trois piliers constituent la base fondamentale de toute stratégie de sécurité des systèmes d'information.

INFORMATION SECURITY PROPERTIES



Autres propriétés importantes de la SSI



Authenticité

Garantie de l'identité des utilisateurs et de l'origine des données pour assurer la confiance dans les échanges d'information.



Non-répudiation

Impossibilité de nier une action effectuée, grâce à des mécanismes comme la signature électronique et l'horodatage.



Traçabilité

Capacité à suivre et enregistrer les actions réalisées sur les systèmes pour permettre des audits et analyses ultérieures.



Le Système de Gestion de la Sécurité de l'Information (ISMS)

ISMS - Information Security Management System

Définition : Système de management permettant d'établir, mettre en œuvre, exploiter, surveiller, réexaminer, maintenir et améliorer la sécurité de l'information.

La norme ISO/IEC 27001

Présentation

- Norme internationale de référence pour la gestion de la sécurité de l'information
- Certification possible par un organisme accrédité
- Basée sur l'amélioration continue (cycle PDCA)

Structure de la norme

1. **Contexte de l'organisation** (Clause 4)
2. **Leadership** (Clause 5)
3. **Planification** (Clause 6)
4. **Support** (Clause 7)
5. **Fonctionnement** (Clause 8)
6. **Évaluation des performances** (Clause 9)
7. **Amélioration** (Clause 10)

Le cycle PDCA appliqué à l'ISMS

Plan (Planifier)

- Établir la politique de sécurité
- Définir le périmètre du SMSI
- Réaliser l'appréciation des risques
- Définir le plan de traitement des risques

Act (Agir)

- Traiter les non-conformités
- Mettre en place des actions correctives
- Améliorer continuellement le système



Do (Déployer)

- Mettre en œuvre les mesures de sécurité
- Former et sensibiliser le personnel
- Gérer les opérations quotidiennes

Check (Contrôler)

- Surveiller et mesurer les performances
- Réaliser des audits internes
- Effectuer des revues de direction

Famille ISO 27000



ISO 27000

Vue d'ensemble et vocabulaire



ISO 27001

Exigences pour le SMSI



ISO 27002

Code de bonnes pratiques



ISO 27003

Lignes directrices pour la mise en œuvre



ISO 27004

Mesure de l'efficacité



ISO 27005

Gestion des risques

Les incidents de sécurité

Définition

Un **incident de sécurité** est tout événement qui :

- Compromet la confidentialité, l'intégrité ou la disponibilité des informations
- Viole les politiques de sécurité établies
- Contourne les mesures de sécurité en place
- Menace la continuité des activités

Types d'incidents de sécurité

1. Incidents techniques

- Attaques par déni de service (DDoS)
- Intrusions dans les systèmes
- Infections par malware (virus, ransomware, trojans)
- Exploitation de vulnérabilités

2. Incidents physiques

- Vol ou perte de matériel
- Accès non autorisé aux locaux
- Destruction ou dégradation d'équipements

3. Incidents humains





- Erreurs de manipulation
- Violations des procédures
- Ingénierie sociale
- Malveillance interne

4. Incidents environnementaux





- Catastrophes naturelles
- Pannes d'infrastructure
- Coupures d'alimentation

Classification des incidents

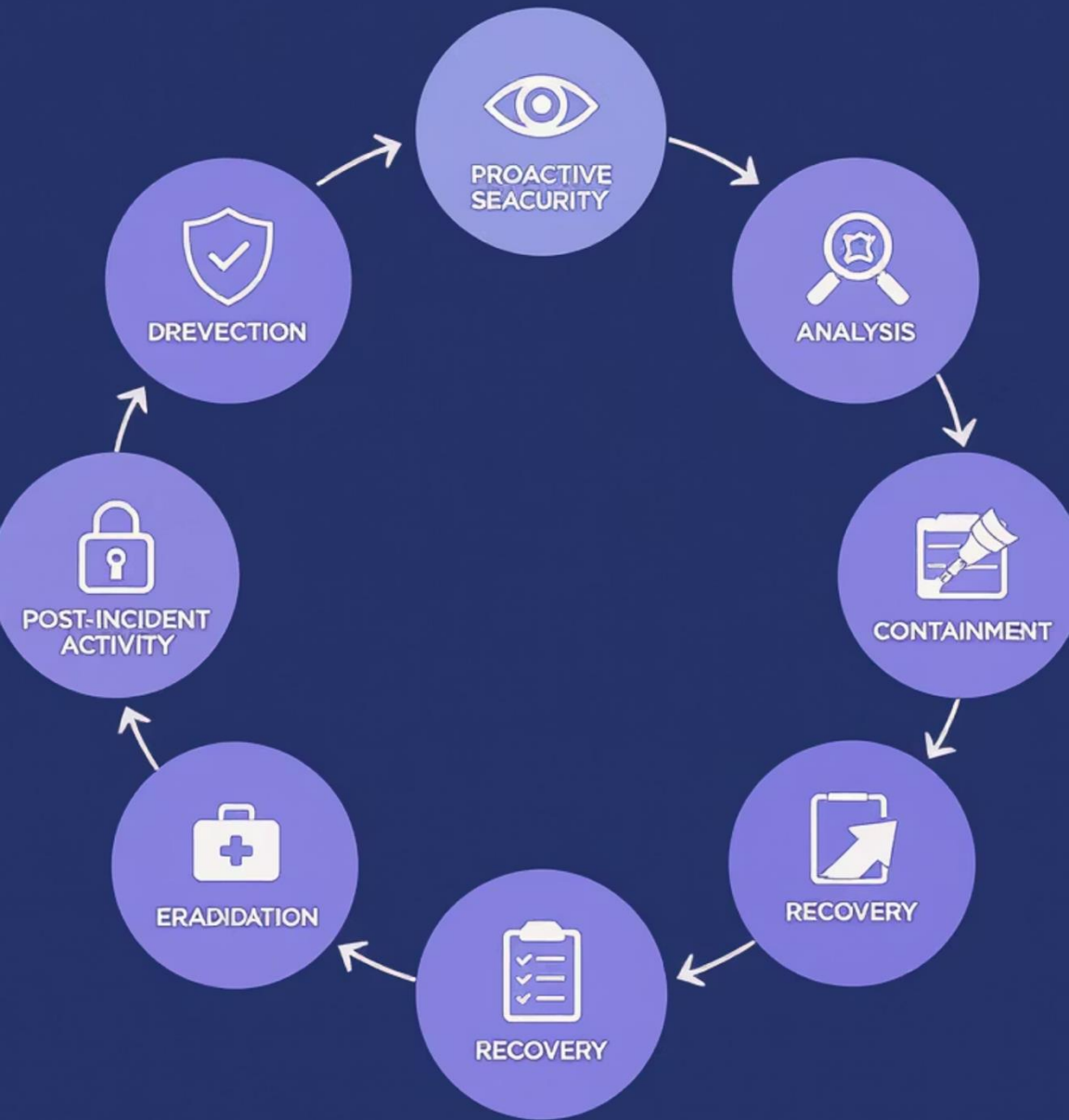
Par gravité

-  **Critique** : Impact majeur sur l'activité
-  **Élevé** : Impact significatif mais gérable
-  **Moyen** : Impact limité
-  **Faible** : Impact négligeable

Par urgence

-  **Immédiate** : Traitement sans délai
-  **Urgente** : Traitement dans les heures
-  **Normale** : Traitement selon les procédures standards
-  **Différée** : Peut attendre

SECURITY INCIDENT LIFECYCLE



Cycle de vie d'un incident de sécurité

Le cycle de vie d'un incident de sécurité comprend plusieurs phases distinctes, de la veille et prévention jusqu'à la résolution complète et le retour d'expérience. Chaque phase joue un rôle crucial dans la gestion efficace des incidents.

Phase 1 : Veille et prévention - Évitement

Définition

Actions proactives pour réduire la probabilité d'occurrence des incidents.



Analyse de risques régulière



Mise à jour des politiques de sécurité



Suppression des vulnérabilités identifiées



Formation continue du personnel



Phase 1 : Veille et prévention - Protection

Définition

Mise en place de barrières pour limiter l'impact potentiel.

Mesures techniques

- Pare-feu et systèmes de filtrage
- Antivirus et anti-malware
- Chiffrement des données
- Contrôle d'accès renforcé

Mesures organisationnelles

- Séparation des privilèges
- Principe du moindre privilège
- Procédures de sauvegarde
- Plans de continuité

Phase 2 : Détection et alertes - Systèmes de détection



IDS (Intrusion Detection System)

- Surveillance passive du réseau
- Détection des comportements anormaux
- Génération d'alertes



IPS (Intrusion Prevention System)

- Détection active avec blocage automatique
- Protection en temps réel



SIEM (Security Information and Event Management)

- Centralisation des logs
- Corrélation d'événements
- Tableaux de bord de sécurité



Encuengy

Emergency Notification

Ennergences and setion for gave yound andrisstangs.



Phase 2 : Détection et alertes - Mécanismes d'alerte

Alertes automatiques

Générées par les systèmes de surveillance et de détection sans intervention humaine, basées sur des règles prédéfinies.

Alertes manuelles

Remontées par les utilisateurs qui constatent des comportements anormaux ou des incidents de sécurité potentiels.

Indicateurs de compromission

IOC (Indicators of Compromise) qui signalent la présence potentielle d'une menace dans les systèmes.

Phase 3 : Réponse et traitement - Traitement initial

Objectifs

- Confirmer la nature de l'incident
- Évaluer l'étendue et l'impact
- Préserver les preuves
- Notifier les parties prenantes

Actions immédiates

- Isolation des systèmes affectés
- Capture des états systèmes
- Documentation des observations
- Activation de l'équipe de réponse

Phase 3 : Réponse et traitement - Confinement

Définition

Actions visant à limiter la propagation et l'impact de l'incident.

Stratégies

- **Confinement à court terme** : Actions rapides pour stopper la propagation
- **Confinement à long terme** : Mesures durables en attendant l'éradication

Techniques

- Déconnexion réseau
- Blocage de comptes compromis
- Modification des règles de pare-feu
- Mise en quarantaine des fichiers suspects

Phase 3 : Réponse et traitement - Acceptation et gestion des risques résiduels

Évaluation

- Analyse coût/bénéfice des mesures
- Identification des risques résiduels
- Documentation des décisions

Options



Acceptation du risque avec surveillance renforcée



Transfert du risque (assurance)



Mise en place de contrôles compensatoires

La réponse à incident - Organisation de la réponse

Équipe de réponse à incident (CSIRT/CERT)

CSIRT : Computer Security Incident Response Team **CERT** : Computer Emergency Response Team

Composition type



Responsable d'équipe : Coordination et décisions



Analystes sécurité : Investigation technique



Administrateurs système : Actions correctives

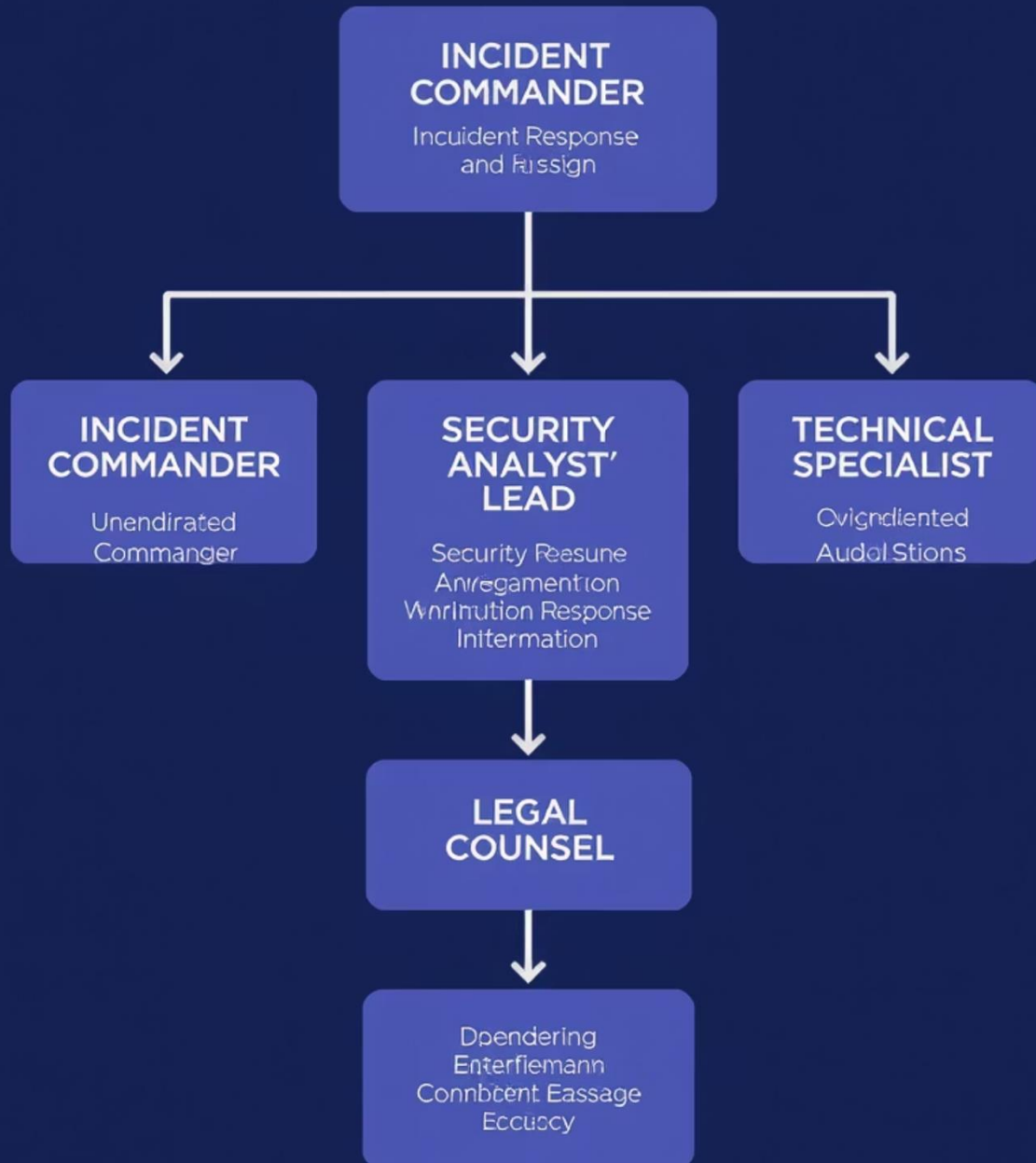


Juriste : Aspects légaux et réglementaires



Communication : Relations internes/externes

INCIDENT RESPONSE TEAM ROLES AND RESPONSIBILITIES



Rôles et responsabilités de l'équipe de réponse



Définition claire des responsabilités

Chaque membre de l'équipe doit connaître précisément son périmètre d'action et ses responsabilités spécifiques lors d'un incident.



Chaîne de commandement établie

Une hiérarchie décisionnelle clairement définie pour éviter les confusions et permettre des prises de décision rapides.



Suppléants identifiés

Des remplaçants désignés pour chaque rôle clé afin d'assurer la continuité des opérations en toutes circonstances.



Formation régulière

Des exercices et formations continues pour maintenir les compétences et la préparation de l'équipe.

Procédures de réponse - Documentation essentielle



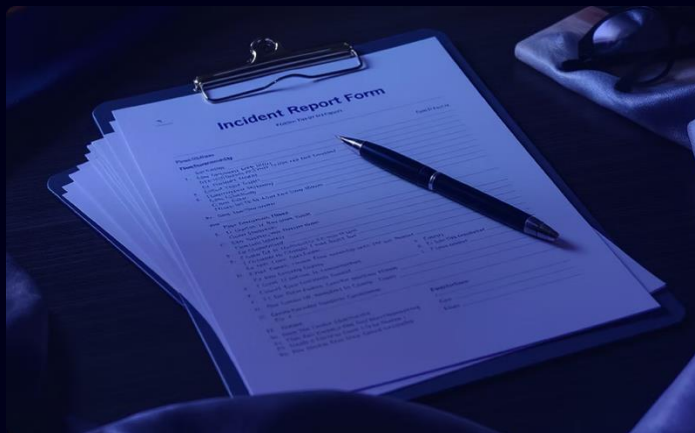
Plan de réponse à incident (PRI)

- Vue d'ensemble du processus
- Rôles et responsabilités
- Coordonnées des contacts clés



Procédures opérationnelles (SOP)

- Instructions détaillées par type d'incident
- Check-lists d'actions
- Outils et ressources nécessaires



Formulaires et modèles

- Rapport d'incident initial
- Journal de bord
- Rapport post-incident



Phases de la réponse

1. Préparation

- Mise en place de l'équipe
- Création des procédures
- Formation et exercices
- Mise en place des outils

2. Identification

- Qualification de l'incident
- Collecte des informations initiales
- Évaluation de la criticité

3. Confinement

- Actions immédiates
- Préservation des preuves
- Communication interne

Phases de la réponse (suite)

4. Éradication

- Suppression de la cause
- Nettoyage des systèmes
- Validation de l'éradication

5. Récupération

- Restauration des services
- Surveillance renforcée
- Validation du retour à la normale

6. Retour d'expérience

- Analyse post-mortem
- Documentation des leçons apprises
- Mise à jour des procédures



Processus d'escalade - Niveaux d'escalade



Niveau 1 - Opérationnel

- Incidents mineurs
- Résolution par l'équipe technique
- Délai : < 4 heures



Niveau 2 - Tactique

- Incidents significatifs
- Implication du management IT
- Délai : < 24 heures



Niveau 3 - Stratégique

- Incidents majeurs/crises
- Cellule de crise activée
- Direction générale impliquée

Critères d'escalade

- Impact sur le business
- Nombre de systèmes/utilisateurs affectés
- Durée de l'incident
- Exposition médiatique potentielle
- Obligations réglementaires

Communication de crise

Communication interne

- Information régulière des équipes
- Mise à jour du management
- Coordination entre services

Communication externe

- Notification aux autorités (ANSSI, CNIL)
- Information des clients/partenaires
- Gestion des relations presse
- Communication sur les réseaux sociaux

Indicateurs et métriques

KPI de performance

MTTD

Temps moyen de détection

Mean Time To Detect

MTTR

Temps moyen de réponse

Mean Time To Respond

MTTC

Temps moyen de
confinement

Mean Time To Contain

MTTE

Temps moyen
d'éradication

Mean Time To Eradicate

Métriques de suivi

- Nombre d'incidents par catégorie
- Taux de récurrence
- Coût moyen par incident
- Efficacité des mesures préventives

Conclusion

La gestion de la continuité d'activité et des incidents de sécurité est un processus complexe nécessitant une organisation structurée, des procédures documentées et testées, une équipe formée et préparée, et une amélioration continue basée sur les retours d'expérience.

Le succès repose sur la préparation, la rapidité de réaction et la capacité d'adaptation face aux menaces en constante évolution.