Incidents

**1. Objet**

**1.1 Finalité**

**1.2 Domaine d'application**

**1.3 Glossaire**

**2. Responsabilité**

**3. Documents**

**4. Exigences de la norme ISO 27001 : 2022**

**5. Déroulement**

**5.1 Rôles**

**5.2 Gestion**

**5.3 Signalement**

**5.4 Évaluation**

**5.5 Réponse**

**5.6 Leçons apprises**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2022 |
| **Page** | **Changement** | **Date** |

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité d’assurer une réponse rapide, efficace, cohérente et ordonnée aux incidents de sécurité de l'information, y compris la communication sur les événements de sécurité de l'information et de diminuer la vraisemblance d’apparition ou les conséquences d’incidents futurs.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Incidents » s’applique à toutes les activités liées à l’identification, l’évaluation, le signalement, la classification, la réponse et les leçons des incidents de sécurité de l’information sur les systèmes et applications de notre organisation.

**1.3 Glossaire**

RSI – responsable sécurité de l’information

Incident (de sécurité de l'information) - événement indésirable et inattendu en matière de sécurité de l'information qui peut compromettre des opérations de l’organisation

SI – sécurité de l’information

Vulnérabilité – faiblesse d’un actif pouvant conduire à un accès non autorisé

**2. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de cette procédure. Il est garant de son application. Il a l’appui du directeur.

**3. Documents**

Descriptions de fonction

Événements de sécurité de l’information

Plan de gestion des incidents

Activités de surveillance

Continuité d’activité

Registre des incidents

Collecte de preuves

Déclaration des événements

Programmes malveillants

Sensibilisation et formation

Vulnérabilités techniques

**4. Exigences de la norme ISO 27001 : 2022**

A.5.24 Planification et préparation de la gestion des incidents liés à la sécurité de l’information

L’organisation doit planifier et préparer la gestion des incidents liés à la sécurité de l'information en définissant, établissant et communiquant des processus, rôles et responsabilités sur la gestion des incidents de l’information.

A.5.25 Évaluation des événements liés à la sécurité de l’information et prise de décision

L'organisation doit évaluer les événements liés à la sécurité de l'information et décider s'ils doivent être catégorisés comme des incidents liés à la sécurité de l'information.

A.5.26 Réponses aux incidents liés à la sécurité de l’information

La réponse aux incidents liés à la sécurité de l'information doit être conforme aux procédures documentées.

A.5.27 Enseignements des incidents liés à la sécurité de l’information

Les connaissances acquises à partir des incidents liés à la sécurité de l'information doivent être utilisées pour renforcer et améliorer les mesures de sécurité de l'information.

**5. Déroulement**

**5.1 Rôles**

Les rôles et les responsabilités pour gérer les incidents sont être déterminés et communiqués aux parties concernées, cf. les Descriptions de fonction.

Les éléments suivants sont pris en compte :

* établir une méthode commune pour signaler les événements de sécurité de l'information, cf. le fichier Événements de sécurité de l’information
* établir les activités et les rôles liés à la gestion des incidents :
  + l'administration
  + la documentation
  + la détection
  + le tri
  + la hiérarchisation
  + l'analyse
  + la communication
  + la coordination des parties intéressées
* établir un processus de réponse aux incidents :
  + évaluer
  + répondre
  + apprendre des incidents de sécurité de l'information
* autoriser uniquement le personnel compétent et formé à traiter la gestion des incidents
* établir la formation, la certification et le développement professionnel continu du personnel d'intervention en cas d'incident

**5.2 Gestion**

Détecter les incidents potentiels c’est identifier les plus importantes vulnérabilités connues afin d’être prêt à réagir de manière appropriée. C’est toujours plus facile de répondre à un incident connu qu’à un incident inconnu.

Séquences liées à un incident : surveiller, détecter, classer, analyser et signaler les événements et incidents de sécurité de l'information.

Les [CERT](https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/) (*Computer Emergency Response Team* - Équipe d'intervention en cas d'urgence informatique) français et le [CSIRT](https://www.cert.ssi.gouv.fr/csirt/intercert-fr/) (*Computer Security Incident Response Team -* Équipe de réponse aux incidents de sécurité informatique) peuvent vous aider pour consulter tout incident connu ou alerte préventive. Les abonnements à des flux RSS (*Really Simple Syndication -* Syndication réellement simple) sont très judicieux pour la veille sur les dernières vulnérabilités connues.

Lorsqu’une vulnérabilité doit être traitée sans délai, elle devient un « incident potentiel ». Plus la réaction est rapide, plus les impacts sont limités.

Le Plan de gestion des incidents prend en compte :

* l'évaluation des événements de sécurité de l'information selon le fichier Événements de sécurité de l'information
* la surveillance selon la procédure Activités de surveillance
* la détection, la classification, l’analyse et le signalement des événements et incidents
* la gestion des incidents jusqu'à leur conclusion, y compris l'activation éventuelle de gestion de crise selon la procédure Continuité d’activité
* la coordination avec les parties intéressées internes et externes comme les autorités, les groupes d'intérêt et forums externes, les fournisseurs et les clients
* l’enregistrement des activités de gestion des incidents dans le Registre des incidents
* le traitement des preuves selon la procédure Collecte de preuves
* l’analyse des causes premières (procédures post-mortem)
* l’identification des enseignements tirés (amélioration des procédures et des mesures)

**5.3 Signalement**

Le signalement inclut :

* les actions à entreprendre en cas d'événement de sécurité de l'information selon la procédure Déclaration des événements
* l'utilisation de formulaires de signalement d'incident
* le retour d'information afin de s'assurer que les personnes signalant des événements de sécurité de l'information sont informées, dans la mesure du possible, des résultats une fois que le problème a été traité et clos
* la création de rapports d'incidents cf. Registre des incidents

Tous les salariés et contractants sont informés de leur obligation de signaler les événements indésirables liés à la sécurité de l’information dans les meilleurs délais au département SI selon le document Déclaration des événements. Cela inclut toute faille de sécurité de l’information observée ou soupçonnée dans les systèmes ou services.

Exemples d’incidents :

* infection d’un virus informatique dans un ordinateur
* panne d’un ordinateur
* dysfonctionnement d’un logiciel
* panne d’un serveur
* défaillance d’un système
* surcharge ou défaillance d'un système d'information critique
* perte, vol, utilisation abusive, endommagement ou destruction d’un actif
* perte d'informations importantes
* changements incontrôlés dans les systèmes d'information critiques, y compris le matériel et les logiciels
* attaque de logiciel malveillant
* panne de la climatisation du local des serveurs
* panne d’alimentation
* impossibilité de se connecter au réseau :
  + interne
  + externe
* personne non autorisée qui cherche à obtenir un accès aux :
  + locaux sécurisés
  + systèmes d'information
  + ressources d'information critiques
* perte ou vol de documents papier contenant des informations personnelles
* inondation ou un incendie
* manque de dispositions adéquates pour la sauvegarde des informations
* copie, modification ou suppression non autorisée de données ou de logiciels
* utilisation non autorisée :
  + des cartes de sécurité d'accès
  + de mots de passe
  + de données
  + de logiciels
* surveillance non autorisée des systèmes d'information, du personnel, des sous-traitants
* divulgation non autorisée d’informations à des destinataires involontaires
* non-respect des politiques, procédures, processus relatifs à la sécurité de l'information

Quand un comportement inhabituel de l'ordinateur est remarqué (soupçon de dysfonctionnement d'un logiciel) suivez les étapes suivantes :

* informez immédiatement le RSI ou son équipe
* cesser d'utiliser l'ordinateur
* n'exécutez aucune commande, y compris les commandes de sauvegarde
* n'essayez pas vous-même de supprimer un virus suspect
* ne fermez aucune fenêtre ni aucun programme
* si possible, déconnectez physiquement l'ordinateur des réseaux

**5.4 Évaluation**

Tout événement indésirable, comportement anormal ou suspecté de l’être est identifié et évalué par l’équipe SI afin de déterminer s'il doit être classé ou non comme incident de sécurité de l'information. Des erreurs humaines, des vols, des pertes ou des défaillances de matériels ne sont pas classées comme incidents mais comme soucis techniques et autres.

Pour évaluer la gravité d’un incident il faut analyser les faits et se poser certaines questions :

* le nombre de postes atteints
* le type d’informations concernées
* le volume d’informations concernées
* le degré de sensibilité des informations
* par où est venu l’attaquant ?
* est-ce que les conséquences incluent :
  + la perte de confiance des clients
  + l’image de l’entreprise
  + des implications financières
* si c’est une perte ou un vol ?
* les informations étaient-elles cryptées ?
* les informations incluaient-elles des données personnelles ?
* si oui, quelles sont ces personnes ?
* quel est le préjudice pour ces personnes

Les applications et les systèmes sensibles disposent d'une fonction automatique de surveillance en cas d'accumulation d'événements anormaux (par exemple tentatives malveillantes infructueuses de connexion ou d'intrusion). Plus de détails dans la procédure Programmes malveillants.

**5.5 Réponse**

L’équipe SI de réponse aux incidents est permanente. La procédure Sensibilisation et formation permet à l’équipe SI d’identifier la formation, la certification et le perfectionnement professionnel requis pour gérer les incidents. Cette équipe sait que réinstaller les systèmes compromis avant d’avoir compris la cause première de l’attaque est une perte de temps et peut s’avérer dangereux.

Les étapes de la réponse sont les suivantes :

* déconnecter l'équipement du réseau, (débrancher physiquement le câble ou la ligne téléphonique) pour empêcher le virus d'accéder aux informations personnelles ou pour attaquer d'autres matériels
* vérifier la mise à jour de l'antivirus et les autres applications de protection (pare-feu et autres)
* gérer la crise selon la procédure Continuité d’activité
* identifier et gérer les vulnérabilités et les faiblesses de la sécurité de l'information, y compris celles liées aux mesures qui ont causé, contribué ou échoué à prévenir l'incident
* réaliser une analyse complète du matériel afin :
  + de déterminer :
    - la cause première
    - le niveau de l'incident
  + d'identifier le programme malveillant
* traiter les failles constatées et les conséquences de l'incident
* recueillir les journaux, enregistrements et autres informations afin :
  + d’analyser les problèmes
  + d’utiliser comme preuve devant un tribunal (rupture potentielle de contrat ou d'exigence réglementaire)
  + de renégocier la rémunération des fournisseurs de logiciels ou de services, si nécessaire
* réinstaller le système
* formater le disque pour être sûr qu'aucun logiciel malveillant ne survive à la réinstallation
* analyser les fichiers sauvegardés afin de vérifier qu’ils ne sont pas infectés
* restaurer les fichiers depuis la sauvegarde
* informer les personnes concernées :
  + de l’incident
  + des actions entreprises
  + des leçons apprises
* signaler l'incident et les mesures prises aux autorités compétentes, si nécessaire (pour des poursuites pénales)
* clôturer l’incident et mettre à jour le Registre des incidents

Recommandations :

* n’ouvrez jamais les pièces jointes non identifiées accompagnant un courriel
* n’installez pas de logiciels sans autorisation
* évitez de surfer sur les sites suspects
* désactiver l'exécution automatique des scripts

**5.6 Leçons apprises**

Les types, les volumes et les coûts des incidents de sécurité de l'information sont quantifiés et surveillés.

Les informations obtenues à partir de l'évaluation des incidents de sécurité de l'information sont utilisées pour :

* améliorer le Plan de gestion des incidents
* identifier les incidents récurrents ou graves et leurs causes afin de :
  + mettre à jour l'évaluation des risques de sécurité de l'information
  + déterminer et mettre en œuvre les mesures supplémentaires nécessaires
  + réduire la vraisemblance ou les conséquences d'incidents similaires futurs
* améliorer la collecte, la quantification et le suivi des informations sur :
  + les types d'incidents
  + les volumes
  + les coûts
* sensibiliser et former le personnel sur :
  + ce qui peut arriver
  + comment réagir
  + comment les éviter à l'avenir

Après chaque incident de sécurité, toutes les personnes ayant participé à la réponse se réunissent pour un retour d’expérience, y compris l’analyse des causes premières.

Les résultats obtenus par l’analyse des incidents de sécurité de l’information passés sont exploités afin de limiter la fréquence des futurs incidents ainsi que les dommages et les coûts associés.

Les conclusions de l’analyse des événements et les décisions prises sont enregistrées dans le fichier Vulnérabilités techniques.