Séparation des environnements

**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**

Historique

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

**1. Objet**

**1.1 Finalité**

La présente procédure a pour finalité de protéger l'environnement de production et les données de toute dégradation par les activités de développement et de test.

**1.2 Domaine d'application**

Le domaine d’application de la procédure « Séparation des environnements » s’applique aux personnes responsables de la séparation des environnements de développement, de test et opérationnels.

**1.3 Glossaire**

SI – sécurité de l’information

RSI – responsable sécurité de l’information

**2. Responsabilité**

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

**3. Documents**

Environnements

Plan de test

Activités de surveillance

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

A.8.31 Séparation des environnements

Les environnements de développement, de test et opérationnels doivent être séparés et sécurisés.

**5 Déroulement**

Le niveau de séparation entre les environnements de production, de test et de développement nécessaire pour prévenir les problèmes de production est identifié et appliqué, cf. Environnements.

Pour imposer un niveau de séparation approprié les éléments suivants sont pris en compte :

* séparer de manière adéquate les systèmes de développement et de production et les exploiter dans des domaines différents (environnements virtuels ou physiques séparés)
* définir, documenter et mettre en place les règles et l'autorisation nécessaire pour le déploiement du logiciel du stade de développement au stade de production
* tester les modifications apportées aux systèmes de production et aux applications dans un environnement de test ou de transfert avant de les appliquer aux systèmes de production selon un Plan de test dédié
* ne pas tester dans des environnements de production, sauf dans des circonstances définies et approuvées
* l’accès aux compilateurs, éditeurs et autres outils de développement ou programmes utilitaires ne sont pas accessibles à partir des systèmes de production lorsqu'ils ne sont pas nécessaires
* afficher les étiquettes d'identification d'environnement appropriées dans les menus pour réduire le risque d'erreur
* ne pas copier d'informations sensibles dans les environnements du système de développement et de test à moins que des contrôles équivalents ne soient fournis pour les systèmes de développement et de test

Dans tous les cas, les environnements de développement et de test sont protégés en tenant compte des éléments suivants :

* correction et mise à jour de tous les outils de développement, d'intégration et de test (y compris les constructeurs, les intégrateurs, les compilateurs, les systèmes de configuration et les bibliothèques)
* configuration sécurisée des systèmes et des logiciels
* contrôle d'accès aux environnements
* surveillance des modifications apportées à l'environnement et au code qui y est stocké
* surveillance sécurisée des environnements
* sauvegardes régulières des environnements

Une seule personne ne devrait pas avoir la capacité d'apporter des modifications à la fois au développement et à la production sans examen et approbation préalables. Ceci peut être réalisé par exemple par la ségrégation des droits d'accès ou par des règles contrôlées.

Dans des situations exceptionnelles, des mesures supplémentaires telles que la journalisation détaillée et la surveillance en temps réel sont mises en œuvre afin de détecter et d'agir sur les modifications non autorisées.

Sans mesures et procédures adéquates, les développeurs et les testeurs ayant accès aux systèmes de production peuvent introduire des risques importants (modification indésirable des fichiers ou de l'environnement système, défaillance du système, exécution de code non autorisé et non testé dans les systèmes de production, divulgation de données confidentielles, problèmes d'intégrité et de disponibilité des données).

Il est nécessaire de maintenir un environnement connu et stable dans lequel effectuer des tests significatifs et empêcher l'accès inapproprié des développeurs à l'environnement de production.

Les mesures et procédures comprennent des rôles soigneusement conçus en conjonction avec la mise en œuvre des exigences de séparation des tâches et la mise en place de processus de surveillance adéquats, cf. la procédure Activités de surveillance.

Le personnel de développement et de test constitue également une menace pour la confidentialité des informations de production. Les activités de développement et de test peuvent entraîner des modifications involontaires des logiciels ou des informations si elles partagent le même environnement informatique.

Séparer les environnements de développement, de test et de production est donc souhaitable pour réduire le risque de modification accidentelle ou d'accès non autorisé aux logiciels de production et aux données métier.

Dans certains cas, la distinction entre les environnements de développement, de test et de production peut être délibérément floue et les tests peuvent être effectués dans un environnement de développement ou via des déploiements contrôlés vers des utilisateurs ou des serveurs en direct (petite population d'utilisateurs pilotes). Dans certains cas, les tests de produits peuvent se produire grâce à une utilisation en direct du produit au sein de l'organisation.

Des processus de support pour l'utilisation des données de production dans les environnements de développement et de test sont nécessaires.