|  |  |  |
| --- | --- | --- |
| logo | Environnements | 1089 |

Responsable :

Mis à jour :

Les environnements de développement, de test et de production sont séparés et sécurisés afin de protéger l'environnement de production et les données de conflits avec les activités de développement et de test.

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

Le niveau de séparation prend en compte les éléments suivants :

* 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 œuvre les règles et l'autorisation 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
* ne pas tester dans des environnements de production, sauf dans des circonstances qui ont été définies et approuvées
* ne pas permettre l’accès aux compilateurs, éditeurs et autres outils de développement ou programmes utilitaires 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 appropriés ne soient fournis pour les systèmes de développement et de test

Les environnements de développement et de test sont protégés et tiennent compte des éléments suivants :

* la correction et la 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)
* la configuration sécurisée des systèmes et des logiciels
* le contrôle d'accès aux environnements
* la surveillance des modifications apportées à l'environnement et au code qui y est stocké
* la surveillance sécurisée des environnements
* les sauvegardes des environnements

Une seule personne ne peut pas apporter des modifications à la fois au développement et à la production sans une revue et une validation préalables. Ceci peut être réalisé par la séparation des droits d'accès ou par des règles spécifiques.

Dans des situations exceptionnelles, des mesures supplémentaires telles que la journalisation détaillée et la surveillance en temps réel sont mises en place 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 comme :

* 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 restrictions incluent des rôles soigneusement conçus en conjonction avec la mise en œuvre des exigences de séparation des tâches et la mise en place de surveillance adéquate.

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.

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.