



Numérique et Cybersécurité

Communication vers les partenaires et clients sur la robustesse du SI

Mettre en Avant les Certificats et Conformités

Pour communiquer efficacement auprès des partenaires et des clients sur la **robustesse du Système d'Information (SI)** et la résilience de l'entreprise, plusieurs points clés peuvent être mis en avant.

Les **certifications de sécurité** obtenues, comme l'ISO 27001, attestent du sérieux de l'entreprise dans la gestion de la sécurité de l'information. Mentionner ces certifications permet de démontrer que les pratiques de sécurité sont conformes aux standards internationaux, renforçant ainsi la confiance des partenaires et clients.

La **conformité aux réglementations** telles que le RGPD et la directive NIS 2 met en évidence l'engagement de l'entreprise envers la protection des données et la sécurité. En soulignant ces points, l'entreprise montre qu'elle adhère strictement aux exigences légales, renforçant ainsi son image de fiabilité et de transparence dans la gestion des données sensibles.

Expliciter les Mesures de Sécurité

La **redondance et la tolérance aux pannes** jouent un rôle central dans la résilience du Système d'Information. Présenter les mécanismes en place, comme l'utilisation de serveurs redondants ou de datacenters géographiquement distincts, démontre que des précautions ont été prises pour assurer la continuité des services, même en cas d'incident majeur.

Les **sauvegardes et plans de récupération** sont également des éléments rassurants pour les partenaires et clients. En communiquant sur la mise en place de sauvegardes régulières et d'un Plan de Reprise

d'Activité (PRA), l'entreprise montre qu'elle est prête à restaurer rapidement les données et à reprendre ses opérations en cas de sinistre, garantissant ainsi une protection efficace des informations essentielles.

Communiquer en toute Transparence

Le **rapport de performance** permet de mettre en avant des indicateurs et statistiques clés qui illustrent la robustesse du Système d'Information. Des données comme le pourcentage de disponibilité du service et le temps moyen de récupération offrent aux partenaires et clients une vue concrète de la fiabilité du SI et de la rapidité de l'entreprise à réagir.

La **gestion des incidents passés** peut aussi être abordée, dans le respect de la confidentialité. Exposer, lorsque cela est possible, des exemples de situations difficiles que l'entreprise a su gérer avec succès renforce l'image de résilience et démontre la capacité à réagir face à des crises.

Un **plan de communication d'urgence** préétabli pour informer rapidement les partenaires et clients en cas d'incident majeur affectant le SI est essentiel. Ce plan doit inclure des messages clairs sur les mesures mises en œuvre pour minimiser l'impact de l'incident, assurant ainsi une gestion transparente et proactive de la situation.

La **transparence** renforce la confiance ; être ouvert sur l'incident, sans divulguer de détails sensibles, montre que des actions concrètes ont été prises pour résoudre le problème. L'objectif de cette communication est de rassurer les partenaires et clients sur la résilience de l'entreprise, en soulignant que la sécurité est une priorité absolue.

En adoptant cette approche, l'entreprise démontre la robustesse de son SI et prouve qu'elle est prête à affronter toutes les éventualités, consolidant ainsi la confiance de ses partenaires et clients.