POLITIQUE DE SECURITE ET DE CONFIDENTIALITE Groupe Everial

La complète satisfaction de nos parties intéressées et leur totale confiance nous sont essentielles.

Dans le prolongement de sa Politique Générale, EVERIAL met en œuvre une politique de sécurité et de confidentialité afin de répondre aux valeurs fortes de l'entreprise.
Cette politique encadre les mesures adaptées aux risques et aux besoins en termes de sécurité pour garantir la confidentialité, l'intégrité et la disponibilité des données traitées dans le cadre des activités de l'entreprise.

Le champ d'application de ces mesures couvre :

- Les informations liées aux phases projet et de réalisation des prestations rendues aux clients
- Les informations traitées dans le cadre du fonctionnement de l'entreprise
- Les données à caractère personnel traitées par Everial en sa qualité de responsable de traitement et de sous-traitant

L'application de ces mesures techniques et organisationnelles se décline sur quatre axes majeurs :

1. La sécurité de notre système d'informations

La sécurité du système d'informations est un enjeu majeur et implique tous les acteurs de l'entreprise.

Les trois piliers de la sécurité sont couverts :

- L'intégrité : garantir que les données, les systèmes et les personnes sont conformes à ce qu'ils doivent être, qu'ils sont cohérents, fiables, et pertinents. Sa mise en œuvre se caractérise par la gestion des mots de passe, la gestion des droits…

- La disponibilité : l'ensemble des mesures mises en œuvre permettent d'assurer la disponibilité des systèmes en fonction des besoins définis. Les domaines de couvertures sont : les réseaux, l'infrastructure, sauvegarde, protection anti-virus et menaces…

- La Confidentialité : garantir que seules les personnes autorisées ont accès aux informations/données correspondantes. La mise en œuvre se fait notamment grâce à la gestion et revue des habilitations.

L'ensemble doit pouvoir être tracé afin de garantir la preuve.

2. La sécurité de nos sites

- Le choix de l'implantation des sites
- Les mesures de protection adaptées
  - ✓ Respect des normes et habilitations électriques
  - ✓ Contrôle d'accès, système anti-intrusion, télésurveillance
  - ✓ Sécurité incendie
  - ✓ Lutte contre les nuisibles
  - ✓ Surveillance de l'environnement de conservation (température, hygrométrie)
  - ✓ Gestion de la maintenance préventive et corrective
- La sécurité des salles serveurs
  - ✓ Double authentification et restriction des habilitations
  - ✓ Dispositifs de sécurité
    - Intrusion (protection par contact, détecteur de présence)
    - Inondation et incendie (alarmes, extinction gaz)
    - Secours électriques (onduleurs, groupe électrogène)
  - ✓ Gestion de la maintenance préventive et corrective des équipements, système de supervision

3. La sélection et l'encadrement de nos collaborateurs

- La sélection des collaborateurs et l'adéquation des compétences
  - ✓ La mise en œuvre d'une politique sociale favorisant la formation continue et tournée vers la motivation et la fidélité des collaborateurs,
  - ✓ La définition des rôles et responsabilités
- Les engagements contractuels de :
  - ✓ Confidentialité
  - ✓ Respect de la présente politique de sécurité et de confidentialité et des documents qui en découlent

4. L'efficacité de nos processus

- Les mesures de gestion des risques et de continuité des activités :
  - ✓ Des analyses de risques pour déterminer les besoins en termes de sécurité
  - ✓ Un Plan de Continuité d'Activités formalise l'ensemble des couples dangers/risques avec les plans d'actions à mener en situation de crise, il est accompagné d'un programme de tests permettant d'évaluer l'efficacité des plans de crise.
- La mise en place d'une organisation transverse intégrant la sécurité des biens et des personnes, du SI et des données à caractère personnel.
- Le contrôle et l'amélioration continue de nos processus conformément aux exigences normatives ISO 9001

Ces mesures sont documentées et maîtrisées par l'application, entre autres, des Politiques, du règlement intérieur, de la charte informatique, des procédures opérationnelles, elles s'appuient également sur la désignation d'un Délégué à la Protection des Données (DPO) et d'un Responsable à la Sécurité du Système d'Informations.

Lyon, le 10/04/2018
Lionel GARCIA