> **Nous envisageons tous les scénarios possibles et les réponses adéquates**

Meridiam

Arnaud Kalika
Directeur de la sûreté du groupe Meridiam

Entreprise française, Meridiam développe, construit et exploite dans le monde entier des infrastructures durables qui améliorent la qualité de vie des populations. Soucieuse de son impact, elle veille également à apporter à ses collaborateurs et parties prenantes le plus haut degré de sûreté et de sécurité.

Quels sont les types de crises auxquelles le groupe Meridiam est le plus exposé ?

Les trois risques dont les probabilités sont pour nous les plus élevées aujourd'hui sont le risque géopolitique (coup d'État, climat insurrectionnel…), le risque médical et le risque d'intégrité. Le sujet est abordé avec la plus grande rigueur, d'autant que nous sommes une société régulée par l'Autorité des Marchés Financiers, soumise à des normes.

Lorsque Meridiam s'est développé au-delà de l'Europe et de l'Amérique du Nord, en 2014, il a fallu adapter les procédures de gestion de crise et de continuité de l'activité. C'est à cette période que nous avons commencé à travailler avec International SOS. Quoi qu'il advienne, le principe central est celui du traitement égal de tous nos salariés, quelles que soient leur fonction ou leur localisation.

Nous avons ainsi établi une procédure « groupe », qui prévoit, par exemple, des audits de sécurité de tous les logements des collaborateurs ou encore la possibilité d'évacuer du personnel, où qu'il se trouve.

Comment se décline localement cette politique groupe ?

Pour chacun des pays où nous sommes présents, nous tenons à jour une liste des risques potentiels précisant l'intensité de chacune des menaces. Au niveau global comme au niveau local, nous envisageons tous les scénarios possibles avec les réponses adéquates, qu'ils concernent les individus, les infrastructures, les aspects informatiques ou les risques financiers comme la corruption ou le blanchiment.

Tout est écrit, rédigé et les scénarios sont régulièrement actualisés. Chacun précise le ou les éléments déclencheurs devant entraîner leur mise en œuvre. Si l'on prend l'exemple de l'Éthiopie, l'un des déclencheurs est la présence de troupes insurgées à une certaine distance de nos bureaux ou de nos actifs.

Que se passerait-il si les communications avec l'une de vos entités étaient coupées ?

Même si les principes directeurs de la gestion de crise sont communs à tout le monde, les entités locales disposent d'un certain degré d'autonomie dans leur application. Par ailleurs, ce cas est prévu. En fonction du pays et du niveau de risque, les bureaux disposent de liaisons satellites. En cas de cyberattaque, les scénarios, les voies de sortie de crise ainsi que des « fiches réflexes » existent également sur papier. Les référents sécurité de chaque bureau ont toujours accès à tous les documents, disponibles sur différents supports.

Comment sensibilisez-vous les collaborateurs à la gestion de crise ?

Notre direction des ressources humaines distille des formations thématiques, dont certaines sont récurrentes et obligatoires tout au long de l'année. Nous effectuons, par exemple, des piqûres de rappel en permanence sur les bonnes pratiques et les bons comportements en voyage. Les collaborateurs sont également sensibilisés aux questions géopolitiques. Pour chacun de nos différents métiers, nous procédons à des exercices de crise destinés à vérifier que les procédures sont connues et maîtrisées. Enfin, la protection de la réputation de l'entreprise passe aussi par des exercices réguliers de communication de crise, destinés à lui permettre de parler d'une seule voix.