BIS CONSULTING
Business Intelligence Security

CATALOGUE DE FORMATION

Sûreté des Biens, des Personnes et de l'Information

Audit | Conseil | Formation | Services | Intelligence économique | Sûreté publique

Le mot du Directeur

Aujourd'hui, la prise en compte de l'intelligence économique par les dirigeants d'entreprises est effective dans son aspect offensif, conscients de leur intérêt à la pratiquer, en revanche l'aspect défensif reste encore trop souvent déficient, faute d'y consacrer le temps, le budget et les moyens nécessaires.

Et lorsque le chef d'entreprise consent à accorder du temps, de l'argent ou d'autres moyens pour protéger son entreprise des agresseurs potentiels, c'est plutôt dans la sécurité physique ou la sécurité des systèmes d'information qu'il investit.

Pourtant, c'est l'individu qui reste plus que jamais le maillon faible dans une organisation. Plus des trois quarts des sinistres informationnels constatés dans les entreprises ou organisations sont le fait de collaborateurs internes trop souvent négligents, étourdis, fautifs ou parfois malveillants, conséquence de la rencontre inopportune avec un concurrent, un client, un fournisseur, un ancien collaborateur, un consultant qui, à votre insu, peut devenir un collecteur d'informations.

Les déplacements de collaborateurs se sont multipliés, la multiplication des échanges par voie numérique et le nomadisme informatique sont autant de situations exposant les détenteurs d'informations sensibles que nous sommes tous, quelle que soit notre position dans la hiérarchie.

L'individu reste toutefois l'acteur essentiel de toute politique ou démarche en matière de sécurité et/ou de sécurité. Aussi, il nous semble utile de vous proposer ce catalogue de formation « Sécurité, sûreté et facteur humain dans les organisations ». Il vise à vous sensibiliser, à vous former, à vous rappeler que la sécurité et la sûreté sont avant tout affaires de bon sens.

Toutes les dispositions prises en matière de sécurité ou sûreté n'auront qu'un effet limité si les personnes concernées ne sont pas régulièrement formées à la sécurité et la sûreté.

Loin de l'image souvent secondaire qui leur est accordée, la sécurité et la sûreté doivent trouver leur place dans la stratégie de l'entreprise ou de l'organisation, pour en améliorer sa performance globale.

Notre offre de formation est un outil de management à disposition des dirigeants visant à responsabiliser et à associer tous les acteurs à cette performance globale de l'organisation.

Nous sommes donc bien loin des espions, des pirates ou autres esprits malveillants. Le salarié, l'employé, le stagiaire, le visiteur, le client, le fournisseur, l'auditeur, le formateur, le consultant, la femme de ménage ou le dépanneur du photocopieur, sont autant d'acteurs potentiellement capables de nuire à votre organisation par la récupération d'informations par opportunité ou naïveté de vos collaborateurs.

Nous espérons que vous trouverez, parmi les formations proposées dans ce catalogue celles que vous recherchez, et qu'elles généreront un intérêt pour votre organisation.

Dans l'attente de vous retrouver bientôt dans nos salles de formation, nous restons à votre disposition pour vous orienter dans vos choix et vous aider à bâtir vos projets de formation.

Yves DECKER

Directeur de BIS CONSULTING

Sommaire

EI001 LES VULNÉRABILITÉS HUMAINES

1 journée

Objectifs :

- Connaître les menaces et les risques pouvant peser sur une organisation du fait des vulnérabilités humaines en interne.
- Mieux anticiper et appréhender les situations à risques par des comportements, des attitudes et des procédures visant à assurer une meilleure protection de l'information dans l'organisation.

Public : Tous publics concernés par la détention et la gestion d'informations dans l'organisation (dirigeants, cadres, chefs de services, personnels administratifs, commerciaux, ingénieurs et techniciens, etc.).

Contenu :

- Définition et qualification de la sûreté des biens, des personnes, et de l'information dans les organisations.
- Présentation et évaluation des menaces et risques pesant sur l'organisation (capteurs d'informations, modes opératoires). Illustration par des cas concrets.
- Identification des vulnérabilités humaines (argent, idéologie, compromission, reconnaissance, bavardages, rencontres, opportunités, négligences, erreurs, vengeances...). Échanges avec les participants, retours d'expériences.
- Études de cas pratiques sur les méthodes utilisées (social engineering…) par les capteurs d'informations (espions, sociétés de renseignement privé, concurrents, lobbyistes, pirates informatiques).
- Identification des risques liés aux hommes de l'organisation en environnement extérieur (salons, foires, colloques, négociations commerciales, expatriation, déplacements...).
- Conseils et règles en prévention et protection des biens, des personnes, de l'information et des systèmes d'information par l'adoption de postures de prudence et de bon sens.

EI002 LE TERRORISME ET SON IMPACT SUR LA SÉCURITÉ ET LA SÛRETÉ DES ORGANISATIONS

1/2 journée

Objectifs :

- Délivrer une information approfondie et actualisée sur les menaces et les modes opératoires terroristes.
- Fournir une meilleure compréhension de la menace terroriste pour l'élaboration des plans de sécurité et sûreté des organisations.

Public : Dirigeants et cadres, DRH, responsables sécurité-sûreté, ingénieurs et techniciens, chefs d'équipe.

Contenu :

- État de la menace terroriste
- Modes opératoires du terrorisme, cibles privilégiées et modes d'actions. Études de cas.
- Prosélytisme et recrutement.

EI003 LA GESTION DES RESSOURCES HUMAINES DANS UN SOUCI DE SÉCURITÉ ET DE SÛRETÉ AU SEIN DES ORGANISATIONS

1/2 journée

Objectifs :

- Connaître les menaces pouvant peser sur une organisation du fait des comportements humains.
- Déterminer les risques liés aux hommes.
- Anticiper les situations à risques par une meilleure maîtrise des ressources humaines.

Public : Dirigeants, DRH et tous publics concernés par le recrutement et la gestion des ressources humaines.

Contenu :

- Définition et qualification de la sûreté des biens, des personnes et de l'information dans les organisations, présentation et évaluation des menaces et risques pesant sur une organisation.
- Identification des vulnérabilités humaines (argent, idéologie, compromission, reconnaissance, bavardages, rencontres, opportunités, négligences, erreurs…). Échanges avec les participants, retours d'expériences.
- Conseils et règles de sécurité et sûreté en matière de gestion des ressources humaines dans une organisation (recrutement, profilage, collégialité de l'embauche, partage des compétences, «besoin d'en connaître», habilitation, responsabilisation, dialogue social, etc.).

EI004 L'INGÉNIERIE SOCIALE

1/2 journée

Objectifs :

- Démontrer combien le facteur humain est le maillon faible de la chaîne de sécurité et sûreté de l'information.
- Délivrer des conseils et méthodes (procédures, pièges anti-manipulateurs) destinés à limiter le risque d'être victime d'ingénierie sociale.

Public : Personnel administratif, standardistes, personnels d'accueil, de communication, de formation, de relations extérieures.

Contenu :

- Définition de l'ingénierie sociale (exploitation des faiblesses du comportement humain).
- Étude des différentes approches psychologiques.
- Identification des vecteurs d'attaque (Internet, téléphonie, approche directe, reverse social engineering, fouille des poubelles).

EE001 L'HOMME ET LES DANGERS DANS SES DÉPLACEMENTS ET VOYAGES

1 journée

Objectifs :

- Former vos personnels en déplacement dans le cadre de leurs missions professionnelles.
- Prévenir les comportements à risque des personnels en fonction de la situation sécuritaire du pays visité (à risque, sensible ou instable) et des Us et coutumes.
- Évaluer les menaces ou situations à risques (criminalité, instabilité politique, conflits ethniques ou religieux, corruption, déstabilisation) pouvant peser sur les personnels.

Public : Dirigeants et cadres, commerciaux, personnels amenés à se déplacer.

Contenu :

- Vulnérabilités des voyageurs (transport, hôtel, restaurant, …) dans le cadre de leur mission, échanges avec les participants, retours d'expériences.
- Approche géopolitique avec problématique de la sûreté dans un cadre international.
- Inventaire des menaces et risques pouvant exister dans le pays d'accueil, atteintes aux personnes et aux informations détenues (supports numériques, documents, discussions).
- Principes de sûreté et sécurité à adopter en cas d'incident ou de crise. Conduites à tenir, méthodes de secours.

EE002 LES ÉXPATRIÉS FACE AUX SITUATIONS À RISQUES

1 journée

Objectifs :

- Former vos personnels et leurs familles expatriés dans le cadre de leurs missions professionnelles dans des pays à risques, sensibles ou en zone de conflit.
- Évaluer les menaces ou situations à risques (criminalité, instabilité politique, conflits ethniques, conflits religieux) pouvant peser sur les personnels et leurs familles dans leurs pays d'accueil.

Public : Tous publics (collaborateurs et leurs familles) concernés par l'expatriation.

Contenu :

- Approche géopolitique avec problématique de la sûreté des expatriés dans un cadre international.
- Inventaire des menaces et risques pouvant exister dans le pays d'accueil des expatriés.
- Vulnérabilités des expatriés dans le cadre de leur mission. Échanges avec les participants, retours d'expériences.
- Principes de sûreté et sécurité à adopter en cas d'incident ou de crise. Conduites à tenir, méthodes de secours.
- Gestion du stress et principe d'adaptation psychologique, sortie de crise.

EE003 INFORMATION ET PROTECTION SUR UN SALON PROFESSIONNEL

1 journée

Objectifs :

- Former vos personnels à l'optimisation de leur participation sur un salon.
- Favoriser les opportunités de collecte d'information dans votre environnement (visiteurs, exposants, …)
- Minimiser les risques et dangers de captation d'informations et de pillage de votre savoir-faire.

Public : Tous publics concernés par les déplacements sur les salons professionnels.

Contenu :

- Définition et qualification de la sûreté des biens, des personnes et de l'information dans les organisations.
- Présentation et évaluation des menaces et risques pesant sur l'organisation (capteurs d'informations, modes opératoires). Illustration par des cas concrets.
- Approche géopolitique avec problématique de la sûreté des personnes en déplacement dans un cadre international.
- Inventaire des menaces et risques pouvant exister dans le pays d'accueil d'organisation du salon professionnel, retours d'expériences.
- Principes de sûreté et sécurité à adopter avant, pendant et après le salon.

MC001 MANAGER SES SERVICES DANS UNE DYNAMIQUE DE PROTECTION DE L'INFORMATION

1/2 journée

Objectifs :

- Former les managers à la prévention des risques et menaces pouvant peser sur une organisation du fait des hommes.
- Donner des méthodes et des outils pratiques de prise en compte des risques et menaces.

Public : Dirigeants et managers.

Contenu :

- Identification et évaluation des richesses internes de l'organisation en matière d'information.
- Établissement de règles, procédures et bonnes pratiques à mettre en œuvre en matière de gestion et protection de l'information.
- Maîtrise des outils de coaching pour le manager.
- Implication et motivation des salariés dans la stratégie de l'entreprise.

MC002 LES MALVEILLANCES HUMAINES DANS LES FRAUDES INTERNES

1/2 journée

Objectifs :

- Former les personnels à la prévention, la détection et l'investigation des fraudes internes.
- Donner des méthodes et des outils pratiques de prise en compte du risque de fraude interne.

Public : Tous publics concernés (auditeurs internes, directeurs sécurité-sûreté, responsables IE, risk manager).

Contenu :

- Identification des méthodes de fraudes internes (corruption, malversation, conflits d'intérêt, détournements, vols).
- Communication de méthodes de détection et d'investigation. Étude de cas, retours d'expériences.

MC003 MANAGEMENT DE LA SÛRETÉ EN ENTREPRISE

2 journées

Objectifs :

- Développer ses capacités managériales.
- Faciliter l'intégration sûreté par les autres fonctions.
- Consolider son expertise sûreté.

Public : Directeurs et responsables sûreté, collaborateurs sûreté, consultants.

Contenu :

- Décision face au risque ou la menace.
- Calcul, analyse et gestion des coûts.
- Démarche de contrôle de gestion.
- Management d'une équipe sûreté.
- Système de Management de Sécurité de l'Information (SMSI).

" Le commissaire aux comptes d'une société de services informatiques, effectuant des contrôles inopinés, tombe par hasard sur une facture de formation émise par une société dirigée par la femme du directeur financier de la société à laquelle il appartient. Le directeur intrigué, décide alors d'ouvrir une enquête qui permettra de mettre en évidence d'autres fausses factures et des retraits en espèce non justifiés d'un montant total de 35.000 euros, sur une durée de 2 ans… "

MC004 L'IDENTIFICATION DES RISQUES ET MENACES ET LA GESTION DE CRISE

1 journée

Objectifs :

- Identifier les risques et les menaces pour anticiper la crise
- Mise en place de dispositifs de gestion de crise.

Public : Dirigeants, DRH, cadres, chefs de services, techniciens et ingénieurs, personnels administratifs.

Contenu :

- Identification des risques de l'organisation (diagnostic, alerte, détecteurs, signaux précurseurs, classification).
- Préparation à la crise (exercices, répétition, simulations, cartographie et définition des types de crises, remontée de l'information).
- Gestion de la crise, identification, mise en place de cellule de crise avec répartition des fonctions à mettre à œuvre, rédactions de procédures et modalités d'activation, animation.
- Logistique de crise, communication de crise et gestion des médias.
- Gestion du stress.
- Retours d'expériences, aspects positifs et négatifs, débriefing.

MC005 LA COMMUNICATION DE CRISE

1 journée

Objectifs :

- Identifier les risques et les menaces pour anticiper la crise.
- Mise en place de dispositifs de gestion de crise.

Public : Dirigeants, DRH, cadres, chefs de services, techniciens et ingénieurs, personnels administratifs.

Contenu :

- Identification des risques de l'organisation (diagnostic, alerte, détecteurs, signaux précurseurs, classification).
- Choix et préparation des communicants de l'organisation.
- Sensibilisation aux types de communication de crise.
- Mise en pratique d'argumentaires adaptés à la culture, l'activité, l'environnement de l'organisation.
- Intégration de la communication dans la gestion de la crise, répartition des fonctions.
- Gestion des acteurs de la crise (médias, pouvoirs publics, salariés, organisations syndicales).
- Retours d'expériences, aspects positifs et négatifs, débriefing.

SI001 LES UTILISATEURS DES SYSTÈMES D'INFORMATION

1 journée

Objectifs :

- Délivrer une information approfondie et actualisée sur les risques et menaces auxquels s'exposent les utilisateurs des systèmes d'information.
- Réduire les comportements à risque.
- Fournir des règles de sécurité et sûreté aux participants.

Public : Dirigeants et cadres, responsables informatique, tous personnels gérant et/ ou utilisant de l'information numérique.

Contenu :

- Panorama de la criminalité informatique (enjeux des agresseurs).
- Identification des menaces et risques pouvant peser sur les organisations.
- Identification des risques et dangers liés aux systèmes d'information (vers, virus, espionnage, hackers, fautes d'employés…)
- Présentation des matériels et démonstration de leurs failles (mails, réseaux sociaux, peer to peer, chevaux de Troie).
- Analyse des modes de communication (réseaux sans fil, accès à distance). Étude de cas.
- Présentation de solutions et de procédures de protection des systèmes d'information (mots de passe, cryptographie, biométrie, antivirus, firewall, droits d'accès limités…).
- Responsabilisation des salariés et employés.

SI002 LE NOMADISME NUMÉRIQUE

1/2 journée

Objectifs :

- Délivrer une information approfondie et actualisée sur les risques et menaces auxquelles s'exposent les utilisateurs d'outils numériques dans leur mobilité.
- Réduire les comportements à risques.
- Fournir des règles de sécurité et sûreté aux participants.

Public : Dirigeants et cadres, commerciaux, personnels amenés à se déplacer.

Contenu :

- Identification des menaces et risques pouvant peser sur les organisations.
- Identification des risques et dangers liés au numérique (appareils nomades, téléphonie mobile, stockage de données, ports USB).
- Présentation des matériels et démonstration de leurs failles.
- Analyse des modes de communication (réseaux sans fil, accès à distance).
- Présentation de solutions et de procédures de protection des personnels et de leur matériel nomade (traçabilité, cryptographie, biométrie).
- Responsabilisation des salariés et employés.

« Faute d'espace, une jeune entreprise a placé au sein de son local d'entretien l'ensemble de ses moyens informatiques déportés. Aussi, lorsqu'un incendie s'y est déclenché en raison de la présence de produits hautement volatiles, ce sont tous les systèmes, mais également l'ensemble des données sauvegardées, qui sont partis en fumée. En absence d'un plan de reprise d'activité, la société a déposé le bilan. »

SI003 LA PROTECTION DES SUPPORTS D'INFORMATION

1/2 journée

Objectifs :

- Former les participants à mieux gérer leurs supports d'information (documents papiers, supports numériques).
- Réduire les comportements à risques.
- Proposer des règles de sécurité et sûreté (habilitation, copies, classification des documents, degré de confidentialité, notion de « besoin d'en connaître »).

Public : Tous personnels.

Contenu :

- Définition de niveaux de risques acceptables (habilitation, copie, « besoin d'en connaître »).
- Définition de règles de classification et confidentialité.
- Principes de sauvegarde des données, stockage et conservation des données, zonage, destruction des données, destruction matérielle des disques durs.
- Plan de continuité d'activité, gestion de sinistre informationnel.
- Responsabilisation des personnes.

SI004 LA PROTECTION DES DONNÉES

1/2 journée

Objectifs :

- Recevoir un aperçu et une connaissance pratique des principales dispositions de la protection des données.

Public : Dirigeants et managers.

Contenu :

- Présentation des textes relatifs à la protection des personnes à l'égard du traitement des données à caractère personnel.
- Le traitement des données à des fins de surveillance sur le lieu du travail :
  - ✓ Les dispositions légales
  - ✓ La mise en œuvre de la loi
  - ✓ Le rôle des autorités de contrôle
  - ✓ Le régime de l'autorisation préalable
  - ✓ Les critères d'appréciation
  - ✓ La preuve de la finalité et de la nécessité du traitement
  - ✓ Le test de la proportionnalité
  - ✓ La prise en considération de la présence de tiers sur le lieu de travail.
- Étude de cas pratiques de la préparation de la demande jusqu'à son dépôt.

SI005 LA CYBERCRIMINALITÉ DANS LES ORGANISATIONS

1/2 journée

Objectifs :

- Délivrer une information approfondie et actualisée sur la cybercriminalité.
- Fournir des règles de sécurité et de sûreté aux participants.

Public : Tous personnels.

Contenu :

- Définition et qualification de la cybercriminalité (piratage informatique, vol d'identité, cyberterrorisme, cybercrime).
- Présentation et évaluation des menaces et risques pouvant peser sur les organisations. Illustration par des cas concrets.
- Conseils et procédures en prévention et protection contre les dangers de la cybercriminalité.

SI006 LES RISQUES ET MENACES LIÉS À L'UTILISATION D'INTERNET

1/2 journée

Objectifs :

- Délivrer une information approfondie et actualisée sur les risques et menaces auxquels s'exposent les utilisateurs d'outils numériques dans leur activité professionnelle.
- Fournir des règles de sécurité et de sûreté aux participants.

Public : Tous personnels ayant accès à Internet dans l'organisation.

Contenu :

- Identification des menaces et risques pouvant peser sur les organisations dans l'utilisation d'Internet par leurs salariés ou employés.
- Inventaire des équipements de sécurité installés sur les postes (antivirus, anti-spywares, anti-spams).
- Dangers des messageries (hameçonnage, social engineering, spams), du e-commerce et des réseaux sociaux.
- Responsabilisation des personnes, engagement contracté.
- Conseils et procédures en prévention et protection contre les dangers de l'utilisation d'Internet dans les organisations.

IE001 LES PRATIQUES D'INTELLIGENCE ÉCONOMIQUE

3 journées

Objectifs :

• Comprendre les pratiques d'intelligence économique et ses enjeux.

• Former les participants à mieux rechercher, traiter, évaluer, capitaliser et protéger les informations qu'ils sont amenés à manipuler quotidiennement, afin d'assurer une efficacité et une rapidité dans la gestion de leurs projets et de leur permettre de prendre les bonnes décisions.

Public : Tous publics concernés par la manipulation d'informations dans l'organisation (dirigeants, cadres, chefs de services, responsables IE, personnels administratifs, commerciaux, ingénieurs et techniciens, etc.).

Contenu :

• Initiation, sensibilisation à l'intelligence économique, ses objectifs et ses enjeux, principes, concepts.

• Comprendre et repérer les vulnérabilités auxquelles peut être exposée une organisation, notamment dans la manipulation de l'information.

• Mise en place d'un plan de veille pour la résolution de problématiques (analyse, mise en place d'indicateurs, recherche de sources pertinentes, collecte, traitement, diffusion).

• Méthodologie et outils de recherche d'informations. Mises en situations, simulations.

• Recherche d'informations hors Internet (sources documentaires, sources humaines, acquisitions en réseau, connaissances internes, rapports d'étonnement, benchmarking).

• Valorisation et diffusion de l'information.

• Mise en place d'un système d'intelligence économique (SIE).

IE002 LA PROTECTION DE L'INFORMATION

1 journée

Objectifs :

• Connaître les menaces pouvant peser sur une organisation.

• Identifier les vulnérabilités internes (humaines, physiques, SSI) et externes (sous-traitance, externalisations, déplacements …).

• Déterminer les procédures et les postures les plus appropriées pour assurer une meilleure protection de l'information au sein de l'organisation.

Public : Tous publics concernés par la détention et la gestion d'informations dans l'organisation (dirigeants, cadres, chefs de services, personnels administratifs, commerciaux, ingénieurs et techniciens, etc.).

Contenu :

• Définition et qualification de la sûreté des biens, des personnes et de l'information dans les organisations.

• Présentation et évaluation des menaces et risques pesant sur l'organisation (capteurs d'informations, modes opératoires). Illustration par des cas concrets.

• Identification des vulnérabilités de l'organisation (échanges avec les participants, retours d'expériences, étude de cas pratiques).

• Identification des risques liés aux hommes de l'organisation en interne comme en externe.

• Conseils en prévention et protection des biens, des personnes, de l'information et des systèmes d'information.

IE003 LE TRAITEMENT DE L'INFORMATION

1/2 journée

Objectifs :

Faire appréhender tous les aspects de la sûreté garantissant la protection d'une donnée ou d'une information quelle qu'en soit sa forme ou son support. La sécurité de l'information n'est confinée ni aux systèmes informatiques, ni à l'information dans sa forme numérique ou électronique.

Public :

Tous publics ayant accès à des informations sensibles et étant concernés par la détention et la gestion d'informations dans l'organisation (dirigeants, cadres, chefs de services, personnels administratifs, commerciaux, ingénieurs et techniciens, etc.).

Contenu :

• Étude du cadre du traitement de l'information au travers du cheminement complet de celle-ci, de sa source à sa destruction, selon le type de données et de support.

• Recherche d'une efficacité opérationnelle globale prenant en compte l'activité de l'entreprise et ses missions pour mieux diriger une politique de gestion des risques.

• Prendre en compte les enjeux juridiques nationaux et internationaux dans le cadre du respect des droits et des valeurs humaines au sein de l'entreprise.

• Appréhender la gestion des menaces, des risques et des dangers visant l'entreprise en respectant les obligations légales.

• Respecter et expliquer les limites liées au traitement de l'information par la communication, la coordination et la définition de domaines de compétence et de responsabilité.

• Aborder le principe du « best practices » par le contrôle qualité, le respect des normes et le processus d'amélioration continue.

• Apporter des éléments d'aide à la prise de décision par l'exploitation statistique, le reporting, la préparation à la situation de crise.

IE004 LE LOBBYING ET LES RÉSEAUX RELATIONNELS OU SOCIAUX

1/2 journée

Objectifs :

- Favoriser les échanges d'informations, et influer sur les prises de décisions.
- Mettre en évidence l'importance de la dimension humaine dans la circulation des informations en réseau.

Public : Publics concernés par la détention et la gestion d'informations et la prise de décisions dans l'organisation (dirigeants, cadres, chefs de services, commerciaux, etc.).

Contenu :

- Typologie de l'information en termes de sources, de valeur, de couleur et de statut.
- Étude du concept de lobbying et de ses dérivés.
- Définition des enjeux de la circulation de l'information en réseau, détermination des acteurs concernés avec leurs signes distinctifs. Étude de cas.
- Cartographie de réseau, évaluation et activation.

" Une société spécialisée dans la maroquinerie de luxe et présente en Afrique se rend compte que le marché y est saturé par de nombreuses contrefaçons à sa griffe. Elle a donc rapidement dû développer des techniques supplémentaires d'authentification de ses produits et faire appel aux autorités gouvernementales afin d'endiguer la distribution de ces faux produits. Par ailleurs, une enquête en intelligence économique a permis de révéler que la filière utilisée pour introduire la contrefaçon dans le pays profitait à des membres éminents du crime organisé en Asie ... "

IE005 LA DÉSINFORMATION ET SA DIMENSION HUMAINE

1 journée

Objectifs :

- Comprendre et repérer les vulnérabilités auxquelles peut être exposée une organisation, notamment par la manipulation de l'information et les techniques de désinformation employées.
- Mettre en évidence l'importance de la dimension humaine dans la circulation des informations en réseau.

Public : Tous publics concernés par la détention et la gestion d'informations dans l'organisation (dirigeants, cadres, chefs de services, personnels administratifs, commerciaux, ingénieurs et techniciens, etc.).

Contenu :

- Typologie de l'information en termes de sources, de valeur, de couleur et de statut.
- Les grands principes de désinformation (action d'influence par incrimination : influencer, nuire, revendiquer, altérer).
- La désinformation : arme politique, médiatique, économique et de guerre. Étude de cas.
- Les concepts associés à la désinformation : propagande, contre-information, guerre de l'information, légende urbaine, rumeur, images rumorales et censure, intoxication, déstabilisation, confiance, lobbying, communication de crise et gestion des risques, procédés journalistiques, groupes de pressions et groupes d'intérêt.
- Définition des enjeux de la circulation de l'information en réseau, détermination des acteurs concernés avec leurs signes distinctifs. Études de cas.
- Moyens de production, de transmission, puis conséquences de la désinformation sur les ressources humaines de l'organisation. Lien RH / ressources matérielles.
- Le comportement humain : facteur décisif de la désinformation.
- Communication interpersonnelle, comportements opportunistes.
- Création, partage capitalisation des ressources papier et numériques dans l'organisation (évaluation, validité de l'information).
- La confiance et son processus de création, notion de coopétition (coopération/compétition).
- Contrôle des flux informationnels.

SO001 LA FONCTION SÛRETÉ

1 journée

Objectifs :

- Connaître la déontologie professionnelle, les lois et décrets d'application pour mieux anticiper et appréhender les situations.
- Savoir gérer un PC Sécurité et les tâches administratives et de reporting qui s'y rapportent.

Public : Tous publics concernés par la fonction sûreté.

Contenu :

- Information sur le cadre légal : code pénal (les conditions d'interpellation, le flagrant délit, la légitime défense, la mise en danger d'autrui, l'atteinte à l'intégrité physique et à la liberté d'aller et venir…) et code civil (le respect de la vie privée et de la propriété privée).
- Présentation d'un poste de sécurité type.
- Les circuits de vérification.
- Savoir rédiger et présenter un compte rendu, des consignes.
- Les techniques d'information et de communication.
- La préparation d'une mission.
- La gestion des clés.

SO002 ACCUEIL ET RÉCEPTION

1/2 journée

Objectifs :

- Faire de la fonction d'accueil, la vitrine et l'image de marque de l'organisation.
- Connaitre les principes de base pour gérer une situation de conflit.

Public : Tous publics concernés par la fonction accueil, responsables sécurité, agents de gardiennage.

Contenu :

- Les missions de l'agent d'accueil.
- L'accueil physique et téléphonique.
- Tenue vestimentaire, élocution, présentation, reformulation, information.
- Comment gérer les comportements agressifs.
- En option sur 1 journée : cas pratique et exercices de mise en situation par jeux de rôle.

SO003 LES SYSTÈMES DE SÛRETÉ ET ACCÈS

1/2 journée

Objectifs :

- Connaitre le principe de fonctionnement des différents systèmes.

Public : Agents de gardiennage.

Contenu :

- Cadre légal et protection des données.
- Le contrôle d'accès : définition du domaine d'application et des modes de contrôle.
- Les systèmes d'alarme et anti-intrusion.
- La vidéosurveillance.
- Les alarmes techniques.
- Le contrôle des rondes de sûreté.

SO004 TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION

1/2 journée

Objectifs :

- Pouvoir rédiger un compte rendu oral et écrit.
- Pouvoir prendre en compte les consignes et leurs mises à jour.
- Pouvoir préparer une mission.

Public : Agents de gardiennage.

Contenu :

- Soigner la description des évènements, des personnes et incidents.
- L'importance du compte-rendu.
- Les consignes : permanentes, ponctuelles, particulières, écrites, verbales.
- Application des consignes selon leur domaine (intrusion, mal-veillance…).
- Notions de base en informatique.

Modalités des formations

Nous proposons différentes modalités de formation : choisissez celles qui s'adaptent le mieux à votre disponibilité.

- **Stage inter-entreprises**
  Formations réunissant des salariés d'entreprises différentes (12 personnes maximum) .
- **Stage intra-entreprise**
  Formations créées en fonction de votre demande et du type du personnel à former. Elles sont traitées au cas par cas, sont modulables selon votre projet et offrent ainsi une formation ciblée. Les formations sur mesure permettent ainsi de répondre à un contexte, des besoins et des objectifs spécifiques. Les formations peuvent être organisées dans vos propres locaux ou dans des lieux extérieurs (12 personnes maximum) .
- **Stage hors temps de travail (HTT)**
  Formations délivrées en soirée et le samedi matin afin de permettre aux individus de concilier vie professionnelle et désir de formation.
- **Séminaires**
  Formations dispensées en journée sur une période de quelques jours.

Calendrier

Lieu et calendrier disponibles en nous contactant :

- Par courrier électronique à **formation@bis-consulting.eu**
- Par téléphone au **+352 (0) 26 51 39 88 / +33 (0) 1 55 70 29 30**

Vous êtes intéressé (e) ?

Pour vous inscrire, contactez nous :
Par courrier électronique à **formation@bis-consulting.eu**
Par téléphone au **+352 (0) 26 51 39 88 / +33 (0) 1 55 70 29 30**

Conditions générales de vente

Les tarifs

Pour chaque modalité de formation, une grille tarifaire est disponible.
Les frais de participation comprennent la documentation et les pauses.
Les repas ne sont pas inclus dans le prix de la formation.

Comment réserver votre place?

- Inscription par l'employeur : le bulletin d'inscription est complété et signé par un membre habilité de votre entreprise ou votre organisme.
- Inscription à titre individuel : le bulletin d'inscription est complété et signé par le stagiaire.

Les inscriptions peuvent s'effectuer par téléphone, télécopie, envoi postal ou par Internet. Toute inscription est confirmée par l'envoi d'un courrier et d'une convocation de stage. Une semaine à dix jours avant la date de la session, une convocation précisant la date et le lieu des cours est adressée au participant. Avant cette date, si le nombre d'inscrits est insuffisant, la session peut être annulée.
Les sessions pouvant être annulées en raison d'un nombre insuffisant d'inscrits, il est déconseillé de prendre à l'avance des billets de transport non échangeables et/ou non remboursables.
En cas d'annulation de la session, ce type de billet ne pourra pas faire l'objet d'une demande de remboursement.

Clôture des inscriptions

Les inscriptions sont enregistrées dans l'ordre de leur arrivée jusqu'à concurrence du nombre de places disponibles dans le stage. Si le nombre est trop élevé, une option pourra être enregistrée sur une autre session.
Tous nos tarifs sont revus en début d'année.

Comment annuler ?

Une demande d'annulation ne donne lieu à un remboursement intégral que si elle parvient par écrit au plus tard dix jours ouvrables avant la date d'ouverture du stage. Passé ce délai, nous nous réservons le droit d'exiger le paiement intégral de la formation.
En cas d'empêchement d'un participant, l'entreprise peut lui substituer un autre collaborateur.
En cas de non-présentation au début du stage, d'absence ou d'abandon en cours de stage, le montant des frais de formation demeure exigible en totalité.
En cas de demande de financement des frais de formation à un organisme tiers, et dans l'hypothèse où celui-ci refuse ou interrompt, pour quelque motif que ce soit, la prise en charge préalablement accordée, l'intégralité des sommes dues devra être payée soit par l'entreprise qui a demandé l'inscription pour un collaborateur, soit par le stagiaire.
Toute annulation dans les dix jours ouvrables avant l'ouverture de la session donnera lieu à une facturation intégrale de la session. Toute annulation avant cette date donnera lieu à une facturation correspondant aux frais de gestion de 50 euros TTC.

BIS CONSULTING FRANCE

4, rue de l'Abreuvoir 92400 Courbevoie - France

Tél : +33 (0) 1 55 70 29 30 - Fax : +33 (0) 1 47 68 81 21

formation@bis-consulting.eu

BIS CONSULTING INTERNATIONAL

10 B, rue des Mérovingiens L-8070 Bertrange - Luxembourg

Tél : +352 (0) 26 51 39 88 - Fax : +352 (0) 26 51 39 89

formation@bis-consulting.eu

www.bis-consulting.eu