Anfh Association nationale pour la formation permanente du personnel hospitalier

Délégation

Formation-action : mise en situation cyberattaque (direction)

Le rôle de la direction de l'établissement dans la gestion de la cybersécurité est central. En effet il lui incombe de piloter les équipes et les moyens mis en œuvre afin d'assurer la sécurité informatique de l'établissement qui dépend d'elle. A cette fin il lui faudra définir un ensemble de règles et de protocoles afin de construire et utiliser une chaine décisionnelle efficace. C'est également elle qui validera les plans d'actions et de réponse sur incident de l'ensemble de ses équipes.

En période de crise elle aura également le rôle crucial de communiquer en interne et en externe et de piloter la crise en priorisant, organisant et contrôlant les efforts de chacun afin de maintenir les activités et de revenir le plus vite a un état normal de fonctionnement.

PUBLIC VISÉ :
↗ Tout agent de la FPH travaillant aux services de direction

ORGANISÉ PAR :
↗ Déméter Santé

NOMBRE DE PARTICIPANTS :
↗ 8 à 16 participants

DURÉE :
↗ 1 jours

PRÉREQUIS :
↗ Aucun

CONTACT :
↗ contact@demeter-sante.fr
06-98-28-88-59

OBJECTIFS

↗ "Comprendre à quoi sert la SSI dans un établissement de santé (protection des données, réputation de l'établissement, continuité des soins)."

↗ "Communiquer efficacement avec le SSI"

↗ "Repérer les acteurs"

↗ "Mettre en place une chaîne décisionnelle efficace"

↗"Connaître les prérogatives de chaque secteur d'activité"

↗"Déployer un plan d'action prédéfini"

↗"Mettre en place un plan de de communication adapté en interne et en externe"

MODALITÉS PÉDAGOGIQUES

↗ Expression guidée par questionnement.

↗ Travail en sous groupes

↗ Apports didactiques et conceptuels.

↗ Echanges

↗Etude de cas, analyse de situations

↗Démonstration, exercices

↗Analyse, démarche réflexive autour du vécu et des situations de travail

PROGRAMME

Comprendre à quoi sert la SSI dans un établissement de santé et plus particulièrement dans son service

- Quelle est aujourd'hui l'état de la menace cyber ?
- Les principes de base de la SSI.
- La direction le centre de planification de la politique SSI.

Communiquer efficacement avec le SSI

- Maitriser le vocabulaire et les lignes directrices de la cybersécurité.
- Les types de cyberattaques et leurs impacts.
- Connaitre les bases de sons SI.
- Méthode de communication.
- Quelques aides à la communication.
- Debriefing et mise en commun.

Repérer les acteurs, mettre en place une chaîne décisionnelle efficace

- Les acteurs qui interviennent sur le SI.
- Les processus de décision et de contrôlent en période normales.
- Les processus de décision et de contrôlent en périodes de crises.
- Mise pratique avec test du processus décisionnel pour une situation normale et une situation de crise.
- Debriefing et retour d'expérience sur le processus décisionnel.

Connaître les prérogatives de chaque secteur d'activité

- Définir les rôles et les responsabilités de chacun vis-à-vis du SI et de ses équipements
- Déployer un plan d'action prédéfini
- Phase 1 : Alerter, mobiliser, endiguer
- Phase 2 : Maintenir la confiance et comprendre l'attaque :
- Phase 3 : Relancer les activité métier et durcir les SI.
- Phase 4 : Tirer les leçons de la crise.
- Mise en situation pratique.
- Debriefing partage d'expérience.

Mettre en place un plan de de communication adapté en interne et en externe

- Connaitre les parties prenantes.
- Mettre aux points les procédures de communications.
- Exemple de communication au cours de chaque phase du plan d'action.
- Mise en pratique rédaction.
- Debriefing partage d'expérience