

TOSA CyberCitizen - Référentiel

REFERENTIEL D'ACTIVITES <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	REFERENTIEL DE COMPETENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	REFERENTIEL D'ÉVALUATION <i>défini les critères et les modalités d'évaluation des acquis</i>	
		MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
1. Le monde de la cybersécurité	Les acteurs de la cybersécurité Distinguer et nommer les différents acteurs institutionnels ou individuels de la cybersécurité afin d'identifier l'interlocuteur adapté.	Test adaptatif TOSA. • QCM, manipulation de logiciels • Scoring mathématique IRT (Item Response Theory)	Le(la) candidat(e) est capable : - de distinguer les différents profils d'attaquants et leurs motivations ; - de nommer les grands acteurs publics et leurs actions ; - d'identifier les interlocuteurs privilégiés au sein d'une entreprise.
	Cibles et impacts d'une attaque Reconnaître les risques et objectifs d'attaquants potentiels dans le but de classifier les différentes zones de risque.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : - de reconnaître les principales catégories de failles ; - d'évaluer les différents impacts potentiels d'une attaque d'entreprise.
	Réagir en cas d'attaque Connaître et appliquer les réflexes à avoir en cas d'attaque avérée ou soupçonnée.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : - de reproduire une procédure de collecte de preuves ; - d'identifier l'interlocuteur et le canal pour avertir de l'attaque.
	Identité numérique et authentification Caractériser un mot de passe fort et maîtriser les outils adaptés afin de se garantir la sécurité de son authentification.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : - de caractériser et connaître l'utilité de mots de passe sécurisés ; - de connaître et savoir utiliser une authentification à 2 facteurs ; - d'utiliser un gestionnaire de mots de passe.

TOSA CyberCitizen - Référentiel

REFERENTIEL D'ACTIVITES <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	REFERENTIEL DE COMPETENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	REFERENTIEL D'ÉVALUATION <i>définit les critères et les modalités d'évaluation des acquis</i>	
		MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
2. La sécurité au bureau	La sécurité du poste de travail Repérer les possibles expositions d'informations afin de limiter au maximum les vecteurs d'attaque possible sur son poste de travail.	Test adaptatif TOSA. • QCM, manipulation de logiciels • Scoring mathématique IRT (Item Response Theory)	Le(la) candidat(e) est capable : - de sécuriser l'accès à ses terminaux électroniques ; - de limiter l'exposition de documents ou informations sensibles.
	L'ingénierie sociale Reconnaître les principales méthodes de manipulation utilisées par les attaquants afin de protéger les données et personnes du facteur humain.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : - de distinguer les vecteurs d'attaque par ingénierie sociale ; - de reconnaître une potentielle tentative de manipulation ; - de réagir et alerter en cas de suspicion.
	Les périphériques amovibles Connaître les risques liés aux périphériques amovibles personnels ou externes pour les manipuler leurs données de façon sécurisée.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : - de sécuriser les informations sur ses périphériques amovibles personnels ; - de manipuler de façon sécurisée des périphériques externes.
	Versions de logiciel et mises à jour Comprendre l'intérêt de sécurité des mises à jour logicielles et savoir les appliquer, afin de maintenir un espace de travail actualisé.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : - d'installer un logiciel issu d'une source de confiance ; - de mettre à jour logiciels et système d'exploitation.

TOSA CyberCitizen - Référentiel

REFERENTIEL D'ACTIVITES <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	REFERENTIEL DE COMPETENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	REFERENTIEL D'EVALUATION <i>définit les critères et les modalités d'évaluation des acquis</i>	
		MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
3. La sécurité en déplacement	La sécurité physique des terminaux Reconnaître les compromissions possibles des terminaux physiques, afin de les sécuriser efficacement en déplacement.	Test adaptatif TOSA. <ul style="list-style-type: none"> • QCM, manipulation de logiciels • Scoring mathématique IRT (Item Response Theory) 	Le(la) candidat(e) est capable : <ul style="list-style-type: none"> - de limiter le risque de vol de terminal ou de données dans les transports ; - de sécuriser ses terminaux dans un environnement nouveau (hôtel, salle de réunion)
	Smartphones et sécurité Connaître et appliquer les bonnes pratiques de sécurité liées aux téléphones portables.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : <ul style="list-style-type: none"> - de sécuriser l'accès aux données et services sur son smartphone ; - de connaître les principes et l'utilité d'une gestion de flotte de mobiles professionnels (MDM).
	Les réseaux sans fils Nommer les risques des réseaux sans fil, pour appliquer les outils et réflexes de sécurité de connexion à des réseaux externes.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : <ul style="list-style-type: none"> - de reconnaître et utiliser un réseau sans fil (Wi-Fi, Bluetooth) sécurisé ; - de connaître l'utilité et savoir utiliser un VPN.
	La surexposition des données Distinguer les potentielles sources de fuite de données lors d'un déplacement externe, afin de limiter la diffusion d'informations sensibles.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : <ul style="list-style-type: none"> - à l'extérieur, de limiter l'exposition de données sensible à l'écrit, à l'oral ou sur écran ; - de limiter les informations sensibles laissées après son départ.

TOSA CyberCitizen - Référentiel

REFERENTIEL D'ACTIVITES <i>décrit les situations de travail et les activités exercées, les métiers ou emplois visés</i>	REFERENTIEL DE COMPETENCES <i>identifie les compétences et les connaissances, y compris transversales, qui découlent du référentiel d'activités</i>	REFERENTIEL D'ÉVALUATION <i>définit les critères et les modalités d'évaluation des acquis</i>	
		MODALITÉS D'ÉVALUATION	CRITÈRES D'ÉVALUATION
4. La sécurité à la maison	L'hameçonnage Savoir reconnaître rapidement une tentative d'hameçonnage afin d'appliquer la mesure adaptée à son traitement.	Test adaptatif TOSA. <ul style="list-style-type: none"> • QCM, manipulation de logiciels • Scoring mathématique IRT (Item Response Theory) 	Le(la) candidat(e) est capable : <ul style="list-style-type: none"> - de connaître les éléments à vérifier à l'ouverture d'un mail ; - de détecter une tentative de hameçonnage ; - de savoir traiter et réagir face à une tentative de hameçonnage.
	Cloud et sauvegarde de fichiers Connaître les applications et utilités des outils de GED et services cloud afin de garantir la continuité des activités.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : <ul style="list-style-type: none"> - de maîtriser les principes de sauvegarde de données et de continuité de l'activité ; - d'utiliser un outil de gestion électronique de documents.
	Les fichiers externes Comprendre les dangers des fichiers externes dans le but de les manipuler de façon sécurisée.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : <ul style="list-style-type: none"> - de nommer les risques liés au téléchargement et l'utilisation de documents externes ; - de reconnaître un fichier potentiellement dangereux.
	Vie privée et protection personnelle Distinguer la frontière de son espace numérique personnel, afin de maintenir sa vie privée protégée en travaillant dans un univers numérique.	Test adaptatif TOSA.	Le(la) candidat(e) est capable : <ul style="list-style-type: none"> - de séparer les usages numériques personnels et professionnels ; - de protéger ses informations personnelles et sa vie privée dans le cadre de son travail.