CENTRE GOUVERNEMENTAL DE CYBERDÉFENSE

IA-02

Identification et authentification (utilisatrices et utilisateurs de l'organisation)

Juill. 2026

Votre gouvernement

Québec

IA

Contrôle de l'identité et de l'authentification

Identification and Authentication

IA-02 — Identification et authentification (utilisatrices et utilisateurs de l'organisation) (PaF-)

Énoncés :

Identifier de façon unique et authentifier les utilisatrices et utilisateurs organisationnels, puis associer cet identifiant unique aux processus agissant en leur nom.

Paramètres :

-

Responsable : OP

Discussion :

Les utilisatrices et utilisateurs organisationnels comprennent les employées, les employés ou les personnes dont le statut est considéré par leur organisation comme étant équivalent à celui d'une employée ou un employé (par exemple, entrepreneures, entrepreneurs et chercheuses et chercheurs invités). L'identification unique et l'authentification des utilisatrices et utilisateurs s'appliquent à tous les accès autres que ceux qui sont explicitement mentionnés dans le contrôle AC-14 et qui s'effectuent dans le cadre de l'utilisation autorisée d'authentifiants de groupe sans nécessiter d'authentification individuelle. Puisque les processus sont exécutés au nom de groupes et de rôles, les organisations peuvent exiger l'identification individuelle de chacune des personnes appartenant à un compte de groupe pour rendre compte en détail des activités qu'elle mène sur le système. Les organisations utilisent des mots de passe, des authentifiants physiques ou la biométrie pour authentifier les identités d'utilisateur, ou encore une combinaison de ces méthodes pour l'authentification multifacteur (AMF). Les justificatifs d'identité et les authentifiants biométriques peuvent à l'occasion être considérés comme étant des renseignements personnels. Afin de considérer le concept de la nécessité du point de vue de la protection de la vie privée par rapport à sa proportionnalité, les organisations doivent collecter juste assez de renseignements personnels pour garantir une authentification précise. L'accès aux systèmes organisationnels est soit local, soit réseau. Par accès local, on entend tout accès à des systèmes de l'organisation, par des utilisatrices ou utilisateurs ou par un processus exécuté en leur nom, effectué par l'entremise d'une connexion directe, sans recours à un réseau. L'accès réseau est tout accès aux systèmes organisationnels, par des utilisatrices ou utilisateurs ou un processus exécuté au nom de ces derniers, effectué au moyen de connexions réseau (c'est-à-dire des accès non locaux). L'accès à distance est un type d'accès réseau qui requiert une communication au moyen de réseaux externes. Les réseaux internes incluent les réseaux locaux et les réseaux élargis. Les RPV chiffrés utilisés pour établir des connexions réseau entre des points terminaux contrôlés par l'organisation et des points terminaux contrôlés par une autre entité peuvent être traités comme des réseaux internes du point de vue de protection de la confidentialité et de l'intégrité de l'information transmise sur ces réseaux. Les exigences d'identification et d'authentification pour des utilisatrices et utilisateurs non organisationnels sont décrites dans le contrôle IA-08.