LES CAHIERS

La cybersécurité

Mode d'emploi

ALTHING

CONSEIL EN SÛRETÉ ET SÉCURITÉ PUBLIQUE

PRÉFACE

La protection des données, et plus largement des systèmes d'information, est désormais devenu un élément incontournable pour toutes les organisations.

La diversité des cyberattaques ne touche plus seulement les particuliers ou les grandes entreprises, elle s'étend aujourd'hui aux administrations, aux secteurs vitaux et tend à mettre en difficulté les acteurs du secteur public, peu sensibilisés et préparés pour y faire face.

En effet, en 2020, 20% des secteurs d'activités touchés par des rançongiciels en France étaient des collectivités territoriales.

C'est pour cette raison que la stratégie nationale de cybersécurité présentée le 18 février 2021 prévoit notamment le financement d'audits de sécurité des systèmes d'information des collectivités territoriales piloté par l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI).

Cibles attractives pour les cybercriminels, les collectivités territoriales sont susceptibles d'héberger nombre de données plus ou moins sensibles et symboliques. Les menaces sont nombreuses et la réalisation d'incidents liés à la sécurité de l'information peut affecter de manière durable l'image de la municipalité et la confiance des administrés.

Au-delà des aspects symboliques et financiers, il en va également de la responsabilité du Maire qui, au regard du Règlement Général sur la Protection des Données (RGPD), est tenu à une obligation de moyen permettant la protection des données personnelles hébergées sur le système d'information de sa Collectivité.

Il apparaît alors primordial de lutter efficacement contre cette problématique, afin de protéger les intérêts de votre commune, mais également ceux de vos administrés qui confient leurs données personnelles à vos services municipaux.

Renaud PROUVEUR
PDG du Groupe SPALLIAN

SOMMAIRE

La sécurité des systèmes d'information

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Les menaces en matière de cybersécurité et les enjeux pour les collectivités territoriales sont de plus en plus importants.

Toute collectivité, peu importe sa taille, utilise un système d'information plus ou moins technique et plus ou moins conséquent. Les données conservées par les municipalités revêtent une importance considérable pour les élus, les services de la collectivités comme pour les administrés.

Il est donc primordial de mettre en place un Système de Management de la Sécurité de l'Information pour contribuer à la diffusion des bonnes pratiques au sein de l'administration et assurer une protection nécessaire des actifs primordiaux de la municipalité (données sensibles, personnelles, programmes politiques, projets internes etc.).

Plusieurs avantages découlent de l'installation d'un tel système :

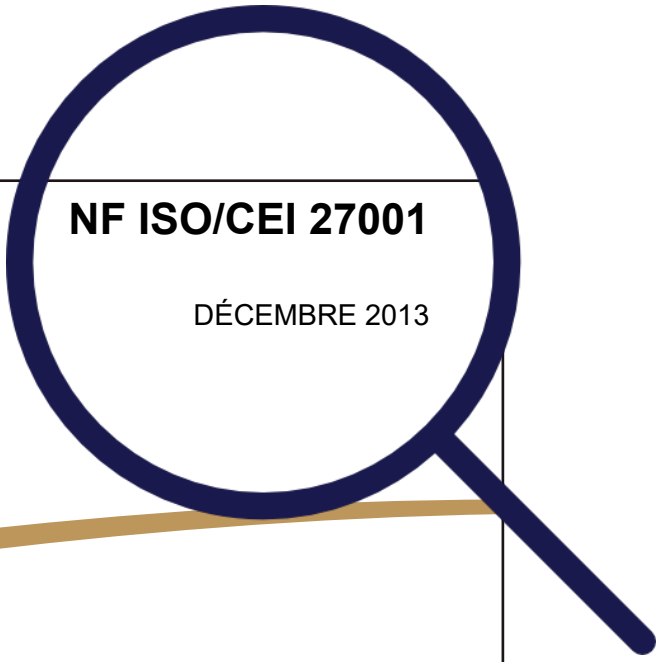
- Conforter son assurance quant à la protection des actifs informationnels,
- Assurer le traitement efficace des risques liés à la sécurité de l'information,
- Mettre en oeuvre des mesures de sécurisation conséquentes et appropriées,
- Assurer l'amélioration continue du système,
- Remplir ses obligations légales et garantir sa conformité réglementaire.

La norme de référence en la matière est la norme internationale ISO/CEI 27001 (Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences). Cette norme présente les grandes lignes et les exigences pour la mise en oeuvre efficace d'un Système de Management de la Sécurité de l'Information (SMSI).

Les principes essentiels découlant de la norme sont les suivants :

- La sensibilisation,
- L'attribution des responsabilités,
- L'engagement de la direction,
- L'appréciation du risque,
- La mise en place de mesures de sécurité concrètes,
- L'intégration de la sécurité comme élément essentiel,
- La prévention et la détection des incidents,
- L'amélioration et le réexamen continu de la sécurité de l'information.

La mise en oeuvre de ces grands principes et des mesures opérationnelles qui en découlent contribue à assurer effectivement la sécurité du système d'information d'une organisation.



NF ISO/CEI 27001

DÉCEMBRE 2013

www.afnor.org

Contacter :
AFNOR – Norm'Info
11, rue Francis de Pressensé
93571 La Plaine Saint-Denis Cedex
Tél : 01 41 62 76 44
Fax : 01 49 17 92 02
E-mail : norminfo@afnor.org

L’évaluation des processus de sécurisation de l’information

L'ÉVALUATION DES PROCESSUS DE SÉCURISATION DE L'INFORMATION SELON LA NORME ISO/CEI 27001

> OBJECTIFS

L'évaluation des processus de sécurisation de l'information a pour objectif de mettre en lumière les carences du système afin d'anticiper la réalisation d'incidents graves liés à la sécurité de l'information.

Lorsqu'une telle évaluation est engagée par une Collectivité, elle permet d'affirmer la volonté de la municipalité de protéger la ville et ses administrés contre les cyberattaques.

Outre la réalisation d'un état des lieux de la sécurité de l'information, l'évaluation permet de mettre en lumière les risques auxquels la commune est exposée, au regard des vulnérabilités identifiées.

> METHODE

L'évaluation du niveau de sécurisation du système d'information, à la lumière de la norme ISO /CEI 27001, passe dans un premier temps par le recensement des données centralisées, et par l'évaluation de leur modalité de traitement.

Il s'agit d'une étape essentielle permettant, notamment, de déterminer les actifs de la Collectivité et de veiller à effectuer une analyse correspondant aux spécificités des données hébergées.

Le respect des obligations légales, contractuelles et la conformité réglementaire doit être analysé. Tout comme doivent être évaluées les politiques internes et le degré de sensibilisation des services municipaux.

La mise en place d'un SMSI

LA MISE EN PLACE D'UN SMSI

> OBJECTIFS

Mettre en place un Système de Management de la Sécurité de l'Information (SMSI) permet d'agir opérationnellement pour la sécurisation de sa commune contre les cyberattaques.

Il s'agit d'un engagement fort qui tend à faire évoluer la gestion du système d'information vers sa sécurisation la plus optimale.

Les éventuels risques identifiés précédemment sont ainsi traités et les menaces existantes sont, quant à elles, anticipées.

> METHODE

La mise en place d'un SMSI passe par un travail collaboratif entre la hiérarchie et les personnes compétentes désignées comme responsables de la mise en oeuvre des différents processus.

Il convient de répondre aux constats effectués par des mesures concrètes, opérationnelles et efficientes.

Cela passe notamment par :

- La rédaction d'une Politique de Sécurité de l'Information,
- La mise en place d'un comité des risques numériques,
- L'élaboration de tous les processus organisationnels conduisant à l'optimisation du SMSI.

Diverses mesures techniques sont ainsi prises pour répondre efficacement et qualitativement aux enjeux de la sécurité du système d'information.

La formation et la sensibilisation des acteurs de la commune

LA FORMATION ET LA SENSIBILISATION DES ACTEURS DE L'ORGANISATION

> OBJECTIFS

La grande majorité des failles et des erreurs concourant à la réalisation d'incidents liés à la sécurité de l'information est dû à l'humain, et plus particulièrement au manque de connaissance et de sensibilisation sur les questions de sécurité de l'information.

Former et sensibiliser ses collaborateurs permet donc d'en faire des acteurs du SMSI à part entière.

Maintenir les compétences, les développer et les mettre à jour en fonction de l'évolution de la menace, permet de limiter considérablement les risques d'exposition aux cyberattaques.

> METHODE

La formation et la sensibilisation des collaborateurs doit passer par différents supports et formats.

Cela doit être réfléchi de manière à toucher tout le monde, sans distinction de poste, dès lors que la personne peut se trouver, à un moment ou à un autre, confrontée à de l'information.

Les temporalités et les modalités doivent être adaptées à la taille de la Collectivité, tout comme à son degré d'exposition aux risques.

Finalement, une veille doit être conduite afin de limiter le risque de ne pas maintenir un niveau de connaissance adapté à l'évolution constante de la menace.

ALTHING

CONTACT

44, rue Chanzy
75011 PARIS

TÉL : +33 (0)1 58 39 30 25

jan.tavart@althing.fr


ALTHING