LES FICHES RÉGLEMENTAIRES CLOUD TEMPLE

L'Esquema Nacional de Seguridad (ENS), en clair

LES FAITS

L'Esquema Nacional de Seguridad (ENS) est le cadre espagnol de cybersécurité pour l'administration électronique. Il est fixé par le Real Decreto 311/2022 du 3 mai 2022. Il s'applique à **toutes les administrations publiques espagnoles**, ainsi qu'à **leurs prestataires privés, y compris étrangers**, dès lors qu'ils traitent des informations ou fournissent des services technologiques (notamment cloud) pour leur compte. L'ENS définit les principes de base, les exigences minimales et les mesures de sécurité que ces systèmes doivent respecter, pour garantir la **confidentialité, l'intégrité, la disponibilité, l'authenticité et la traçabilité** des informations traitées.

LE CONTEXTE

La réforme de 2022 s'inscrit dans le **Plan national de cybersécurité espagnol**, doté d'un milliard d'euros, et dans le Plan de relance post-Covid financé par l'UE. Elle vise à moderniser un dispositif conçu en 2010 face à la sophistication croissante des menaces, et à mieux articuler l'ENS avec les textes européens **NIS2 et DORA** — le Centre Cryptologique National (CCN) publiant des guides de correspondance croisée pour limiter la duplication des contrôles entre référentiels nationaux et européens.

NIVEAU DE SÉCURITÉ	QUI EST CONCERNÉ, QUELLES EXIGENCES ?
Básica	**Systèmes à faible enjeu (sites vitrines, services d'information basique).** Auto-évaluation, sans audit externe. Concerne les services publics dont une atteinte à la sécurité n'aurait qu'un impact limité. Une quarantaine de mesures de sécurité à mettre en œuvre. L'entité ou son prestataire déclare lui-même sa conformité, sans passer par un audit indépendant.
Media	**La majorité des prestataires cloud et éditeurs SaaS qui traitent des données courantes de l'administration (état civil, subventions, portails de démarches).** Certification obligatoire, audit renouvelé tous les 2 ans. S'applique dès qu'une atteinte à la sécurité aurait un impact significatif sur les usagers ou le service. Une soixantaine de mesures exigées. La conformité doit être vérifiée par un audit externe mené par un organisme de certification accrédité, et renouvelée tous les deux ans.
Alta	**Administrations et prestataires qui gèrent les données les plus sensibles ou des infrastructures critiques (santé, défense, ordre public, services essentiels).** Certification obligatoire, contrôle continu. S'applique quand une atteinte à la sécurité aurait des conséquences graves — pour les personnes, pour un service essentiel ou pour la sécurité nationale. Plus de 70 mesures exigées, audit renforcé, et obligation d'utiliser des produits de sécurité qualifiés par le Centre Cryptologique National (CCN), l'autorité espagnole de cybersécurité.

L'ANALYSE

Giuliano Ippoliti
directeur cybersécurité de Cloud Temple

Viser la catégorie Alta, c'est nous donner la possibilité de répondre à l'ensemble du marché public espagnol, y compris ses usages les plus sensibles, plutôt que de nous limiter à une partie de l'offre. C'est une façon de compléter notre couverture européenne de la conformité, aux côtés du SecNumCloud en France, et d'ouvrir la discussion avec des clients et partenaires espagnols en recherche d'un cloud souverain répondant à leurs propres exigences nationales.

MISE EN ŒUVRE ET CALENDRIER

- 2010 → 2022 : premier ENS (RD 3/2010), puis réforme complète par le RD 311/2022
- 24 mois après publication : délai de transition accordé aux entités pour migrer de l'ENS 2010 vers l'ENS 2022
- Tous les 2 ans : renouvellement obligatoire de l'audit pour les catégories Media et Alta
- À suivre : articulation encore à préciser avec le futur schéma européen EUCS

CLOUD TEMPLE