# RAPPORT D'ACTIVITÉ 2022

Ils ne savaient pas que c'était impossible,
alors ils l'ont fait.

AMSN · Sécurité Numérique
PRINCIPAUTÉ DE MONACO

# EDITO

Il convient de remercier en premier lieu les femmes et les hommes qui, par leur implication, permettent de réaliser une transition numérique de la Principauté dans de bonnes conditions de sécurité. La Délégation Interministérielle chargée de la Transition Numérique (DITN), les services de l'État et les Opérateurs d'Importance Vitale sont fortement engagés dans cette transition contrôlée.

Ma gratitude va aux agents de l'AMSN qui sont engagés avec dévouement au quotidien pour accompagner les différentes parties prenantes dans la sécurisation de leurs systèmes d'information.

L'année 2022 a vu apparaître un nouveau conflit armé avec des ramifications non négligeables dans le monde numérique. Des groupes d'activistes se sont créés, se sont affiliés à un camp ou un autre, ont réalisé des attaques au nom d'une cause et certains ont une proximité avérée avec des acteurs étatiques. L'Ukraine a été victime de nombreuses attaques polymorphes, les ex-pays du pacte de Varsovie et les pays baltes sont sous tension et des débordements ont été observés sur d'autres pays européens, notamment sous la forme d'attaques par saturation des sites internet (Italie, France, Norvège, ...)

La maturité de la Principauté en matière de sécurité numérique n'a pas été évaluée par l'Union Internationale des Télécommunications (UIT) en 2022 mais le sera en 2023. Pour autant, deux indicateurs simples permettent de confirmer que le niveau de maturité en matière de cybersécurité des services de l'État et des Opérateurs d'Importance Vitale continue d'augmenter : alors que le nombre d'événements de sécurité a augmenté de 100% en 2022, le nombre d'événements ayant nécessité l'intervention de l'AMSN a lui baissé de 63%. Néanmoins, les Petites et Moyennes Entreprises, qui constituent une grande partie des employeurs de la Principauté, restent encore fragiles. Il conviendra, avec le soutien de la Délégation Interministérielle chargée de la Transition Numérique et du Gouvernement, de prendre des mesures pour accompagner les PME dans la sécurisation de leurs systèmes d'information.

Cette cinquième édition du rapport d'activité présente le bilan du travail réalisé sur l'année 2022 par l'AMSN, les services exécutifs de l'État et toutes les parties prenantes engagées dans la sécurité numérique, et propose des orientations qui permettront de continuer à rehausser le niveau de maturité de la Principauté en matière de sécurité numérique.

Frédéric FAUTRIER
*Directeur*

# LES FAITS MARQUANTS DE 2022

## JANVIER

### CAMPAGNE D'EXPLOITATION DE LOG4SHELL... LA SUITE...

Log4j est une bibliothèque logicielle en source ouverte qui permet de générer des journaux d'événements et des historiques d'applications. Elle est très largement utilisée sur les sites web et intégrée dans de nombreux logiciels dans le monde. Une vulnérabilité critique concernant Log4j a été dévoilée le 10 décembre 2021 ouvrant la porte à une campagne de tentatives d'exploitation particulièrement active en janvier 2022. Elle a eu des effets de bord tout au long du premier semestre de l'année.


## 21 MARS

### PWC RENOUVELLE SA QUALIFICATION PASSI

En présence de Philippe Trouchaud, Partner PwC France, le Directeur de l'AMSN a remis le 21 mars, le nouveau diplôme de Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) à Frank Vanhal, associé PwC Monaco et Stefan Thibault, Directeur Cybersécurité chez PwC.
PwC a reçu pour la première fois cette qualification en Principauté dès 2019 et renouvelle pour une durée de trois ans sa capacité à effectuer des audits qualifiés des systèmes d'information.
Implantée en Principauté depuis plus de 15 ans, et forte de 12 auditeurs certifiés PASSI, PwC accompagne la sécurisation des projets majeurs de transition numérique en Principauté.


## 3 MAI

### RENCONTRE AVEC MONACO BOOST

Le Directeur de l'AMSN a rencontré des entrepreneurs du Monaco Boost afin d'aborder avec eux les problèmes liés à la cybersécurité et les mesures qui peuvent être mises en œuvre pour réduire les risques.

Monaco Boost est une pépinière d'entreprises, qui permet de faciliter et d'accélérer la création et le développement d'entreprises en Principauté pour les activités nouvellement créées par des entrepreneurs monégasques.


## 4 MAI

### DELOITTE RENOUVELLE SA QUALIFICATION PASSI

Le 4 mai, a eu lieu la remise officielle par le Directeur de l'Agence Monégasque de Sécurité Numérique du diplôme de Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) à Pierre-Alexis Saint-Michel, Associé Cybersécurité de Deloitte Conseil et à Julien Le Marrec, Directeur de Deloitte Monaco. Le renouvellement de la qualification de ce cabinet international confirme l'engagement à Monaco de l'un des leaders du conseil et de l'audit, largement reconnu dans les différents domaines de la cybersécurité.


## 5 MAI
### RENCONTRE AVEC LE CSIRT-PJ

Le centre de réponse aux incidents de l'AMSN (CERT-MC) a rencontré son homologue de la Police Nationale française.
La division de l'anticipation et de l'analyse, une des équipes de l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), mène une surveillance proactive sur les phénomènes de cybercriminalité et fournit une analyse technique hautement qualifiée aux services opérationnels en charge des enquêtes judiciaires.
Centre de réponse aux incidents de la police judiciaire (CSIRT-PJ), elle développe à ce titre des partenariats d'échange d'informations et de prévention du risque cyber avec le secteur privé.


## 12 MAI
### RENOUVELLEMENT DE MONACO CARE SAFETY

Depuis 2019, l'État finance une solution de sécurité développée par la société finlandaise F-Secure et mise en œuvre par Monaco Telecom.
L'engagement de l'État dans la cybersécurité permet à tous les clients de Monaco Telecom, résidents et entreprises, ayant souscrit un accès internet de bénéficier gratuitement d'un antivirus, d'un navigateur sécurisé et d'un contrôle parental. La solution peut être utilisée sur PC, MAC, smartphone Android et iPhone et peut être installée simultanément sur 10 terminaux sans frais.

## 23 MAI
### L'AMAF ACCUEILLE L'AMSN

Le Bureau de l'Association Monégasque des Activités Financières, présidé par Monsieur Etienne Franzi, a reçu le Directeur de l'AMSN.
Ce point d'étape a permis de présenter le niveau de maturité en matière de sécurité numérique du secteur bancaire constitué de 14 banques de droit monégasque et 11 agences ou succursales de banques étrangères. Les félicitations ont été adressées à l'ensemble des banques pour le travail accompli dans un contexte géopolitique et pandémique particulièrement difficile.

## 24 MAI
### RÉAMÉNAGEMENT DU «SECURITY OPERATIONS CENTER»

Ouvert le 17 mars 2020, le centre de supervision de la cybersécurité (SOC) de l'AMSN, a fait l'objet d'un réaménagement en 2022.
Ces travaux étaient nécessaires pour accueillir de nouveaux ingénieurs avec pour objectif courant 2023 d'étendre les plages d'ouverture du SOC aux samedis et dimanches. Deux positions de travail ont été ajoutées. Le SOC est ouvert actuellement les jours ouvrés, de 07h30 à 21h30.


## 26 JUIN AU 1ER JUILLET

### CONFÉRENCE ANNUELLE DU FIRST

Le Forum of Incident Response and Security Teams (FIRST), association qui regroupe 635 équipes de sécurité de 101 pays a organisé sa conférence annuelle à Dublin. L'AMSN, qui est membre du FIRST depuis 2018, y était représentée par son Directeur et le responsable de l'équipe de réponse aux incidents de sécurité informatique de l'AMSN (CERT-MC).

## 27 AU 30 JUIN

### L'AMSN PARTICIPE AU CTF ORGANISÉ PAR LE FIRST

Le FIRST organise chaque année un exercice « Capture The Flag » (CTF). Le CTF consiste en une série de challenges techniques pour lesquels les participants doivent trouver une réponse afin de solutionner ces défis (Flag). Chaque drapeau soumis contribue au score de l'équipe. L'AMSN a terminé 7ème sur les 91 équipes engagées.

## 12 JUILLET

### LE CERT-MC ACCRÉDITÉ PAR TRUSTED INTRODUCER

L'équipe en charge de la réponse aux incidents de sécurité informatique de l'AMSN (CERT-MC), évaluée par Trusted Introducer, a été accréditée le 12 juillet 2022 auprès de la TF-CSIRT, force d'intervention regroupant les CSIRT. Cette accréditation est la reconnaissance des méthodes de travail et du savoir-faire du CERT-MC, créé en 2016 au sein de l'AMSN. La TF-CSIRT regroupe 488 équipes de réponse à incidents, réparties sur 71 pays, parmi lesquelles 46 sont certifiées, 239 accréditées et 174 simplement listées. Le CERT-MC met tout en œuvre pour atteindre la certification à l'horizon 2025.

## 22 JUILLET

### LSTI CERTIFICATION REMET SES RAPPORTS D'AUDIT À L'AMSN

LSTI, Organisme d'évaluation de la conformité accrédité par le COFRAC (Comité français d'accréditation), inscrit sur la liste officielle de la Commission Européenne pour réaliser les audits de certification des Prestataires de Services de Confiance (PSCo), a remis à l'AMSN les rapports d'audit des premiers candidats à la délivrance de signatures électroniques et/ou de cachets électroniques.
Prévue par la loi n°1.383 du 2 août 2011 pour une Principauté numérique, modifiée fin 2019, la qualification des Prestataires de Services de Confiance de la Principauté permet de renforcer la confiance des utilisateurs dans les services numériques qu'ils leur proposent.
L'AMSN, organe de contrôle de la Principauté en la matière, est en mesure de délivrer la qualification sur la base d'un audit réalisé par un organisme d'évaluation de la conformité.

## 13 SEPTEMBRE
### QUALIFICATION PSCO DES SERVICES PUBLICS

La Mairie, la Direction de la Sûreté Publique, la Direction de l'Expansion Economique, la Direction des Ressources Humaines et de la Formation de la Fonction Publique et la Direction des Services Numériques, ont reçu leur diplôme de qualification en tant que Prestataires de Services de Confiance (PSCo) pour la délivrance de certificats de signatures électroniques et/ou de cachets électroniques en présence de Monsieur Patrice Cellario, Conseiller de Gouvernement – Ministre de l'Intérieur et Président du Comité de Suivi des Services de Confiance.

## 28-29 SEPTEMBRE
### 67ÈME RÉUNION DE LA TF-CSIRT

A l'occasion de la 67ème réunion de la TF-CSIRT, qui se déroulait à Vilnius, en Lituanie, coincée entre la Biélorussie et l'enclave Russe de Kaliningrad, le Directeur de l'AMSN et le Responsable du CERT-MC ont bravé les éléments pour assister aux présentations de leurs pairs.
Les conséquences cyber du conflit Russo-Ukrainien ont été abordées par les représentants des CSIRTs des pays d'Europe de l'Est frontaliers du « théâtre des opérations ».


## 12 OCTOBRE
### SAS LE PRINCE ALBERT II AUX ASSISES DE LA SÉCURITÉ

A l'occasion de la 22ème édition des Assises de la sécurité qui se déroulait au Grimaldi forum du 12 au 15 octobre, le Prince Albert II de Monaco, accompagné de SEM le Ministre d'État et du Conseiller de Gouvernement – ministre de l'Intérieur, a rencontré plusieurs entreprises spécialisées dans le secteur de la sécurité numérique.

Parmi elles, étaient présentes les entreprises monégasques Monaco Cyber Sécurité, MVE, Smart Global Governance, KPMG, PwC, Lutessa, Luxtrust, Pineappli, et Monaco Telecom.

## 13 OCTOBRE
### PREMIÈRE ENTREPRISE MONÉGASQUE QUALIFIÉE PSCO

Le Directeur de l'AMSN a remis à Jean-Marc RIETSCH, Président fondateur de Pineappli, le diplôme de qualification de Prestataire de Service de Confiance pour le service d'archivage électronique Pineappli. Pineappli devient la toute première entreprise privée monégasque à obtenir ce statut de la part de l'AMSN. Le système d'archivage électronique de Pineappli répond à l'ensemble des très hautes exigences fixées par le cadre règlementaire pris en application de la loi n°1.383 pour une Principauté numérique. Cette qualification consacre le travail et la rigueur de Pineappli, startup monégasque retenue en 2020 par MonacoTech, incubateur de la Principauté, et apporte la preuve que les procédés de sécurité appliqués aux données de ses clients sont particulièrement fiables et pérennes. Pineappli avait déjà obtenu plusieurs certifications ISO 27001, HDS, eIDAS dès 2021 et NF 461 par Afnor Certification en mars 2022.

# LES CHIFFRES CLÉS 2022

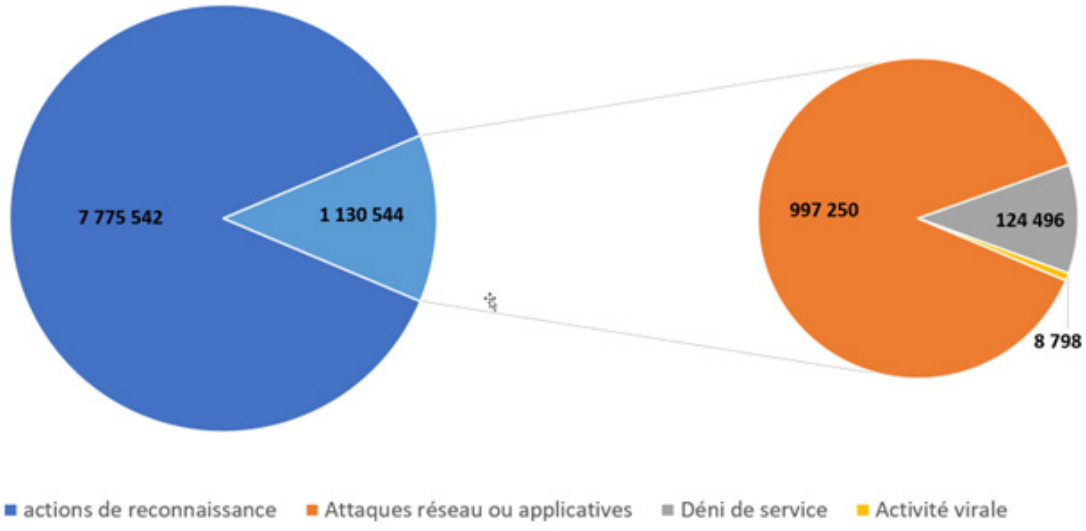
## L'AMSN

**3** nouvelles recrues en 2022.
**14** personnes au 31 décembre 2022.

**7%** de femmes.
**93%** d'hommes.
**38** ans d'âge moyen.
**1,3** millions d'euros de budget pour les moyens de l'AMSN.
**4,8** millions d'euros de budget sécurité numérique pour les services exécutifs de l'État.
**68** Opérateurs d'Importance Vitale.

## LES ÉVÉNEMENTS DE SÉCURITÉ SUR LE PÉRIMÈTRE ÉTATIQUE

L'AMSN a comptabilisé en 2022, en amont des logiciels et matériels de sécurité de ses parties prenantes étatiques, 9 millions d'événements de sécurité. Parmi eux, apparaissent 7,8 millions d'actions de reconnaissance, et 1,1 million de tentatives d'attaques ou d'utilisation d'outils malveillants destinés à les commettre. Des dénis de service ont notamment été tentés par les attaquants.




Sur **1,1 million** de tentatives d'attaques visant les entités de l'Etat en 2022 :

- 672 événements ont fait l'objet d'un suivi avec les entités concernées **↗+71%.**
- 7 événements ont nécessité des investigations approfondies par le CERT-MC **↘-23%**.

## LE TOP 5 DES TECHNOLOGIES VULNÉRABLES CIBLÉES

Sur le périmètre qu'elle supervise, l'Agence a comptabilisé en 2022 de nombreuses tentatives d'exploitation de vulnérabilités. Etaient principalement concernés :

1. La bibliothèque **Log4j,** utilisée dans de nombreux logiciels, qui a été la vulnérabilité la plus exploitée en 2022.
2. Le langage de programmation **PHP**, principalement utilisé pour produire des pages web qui a fait l'objet de nombreuses tentatives d'exploitation sur diverses vulnérabilités répertoriées.
3. Les équipements informatiques «grand public» (**Dlink, Zyxel, Mikrotik**, etc.) qui sont des cibles faciles pour les attaquants car généralement peu maintenus.
4. Les serveurs Web **Apache**.
5. Les serveurs de mail **Zimbra**.

## LES RISQUES CONSTATÉS EN PRINCIPAUTÉ

L'Agence répertorie chaque semaine la totalité des serveurs informatiques de la Principauté qui utilisent des protocoles de communication non sécurisés ou qui ont des vulnérabilités exposées sur Internet. Dans les deux cas, leurs propriétaires prennent des risques pouvant entraîner le vol de leurs données, la prise de contrôle de leurs serveurs par des attaquants, ou encore un rançonnement.
**712** serveurs informatiques ont utilisé des protocoles de communication non sécurisés **↗+71%**.
**1132** serveurs ont exposé des vulnérabilités exploitables. **↗+82%**.

## LA CYBERCRIMINALITÉ

La Direction de la Sûreté Publique contribue à la cybersécurité en exerçant le volet répressif des dispositions prévues par la loi et les accords internationaux.
Forte d'une unité spécialisée dans la lutte contre la criminalité technologique, elle a été amenée en 2022 à apporter assistance aux victimes et à intervenir dans le cadre d'instructions de la Justice sur de nombreux dossiers :

- **2** rançongiciels.
- **5** intrusions dans des systèmes d'information.
- **1** manipulation de compte bancaire opérée en ligne.
- **1** vol de données au travers de sites web ou annonces frauduleux.
- **2** escroqueries par courriels frauduleux.
- **1** escroquerie par usurpation d'identité sur les réseaux sociaux.
- **3** escroqueries par site web ou annonces frauduleux.
- **1** escroquerie par faux ordre de virement via courriel.
- **4** infractions liées aux cryptomonnaies.
- **2** usurpations d'identités sur des réseaux sociaux.
- **1** diffamation sur des réseaux sociaux.
- **1** diffamation par courriel.

## RÈGLEMENTATIONS MONÉGASQUES PUBLIÉES EN 2022

**5 textes règlementaires dans le domaine de la sécurité numérique** ont été publiés en 2022, parmi lesquels l'arrêté ministériel n° 2022-331 du 13 juin 2022 portant application de l'article 23 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, définissant l'organisation de la sécurité des systèmes d'information au sein des services exécutifs de l'État et fixant les mesures de sécurité applicables.

## FORMATION-INFORMATION-SENSIBILISATION

**20** formations en ligne ont été suivies par les Agents de l'AMSN.
**4** sensibilisations à l'accès aux informations classifiées ont été dispensées par l'AMSN.
**244** « actualités » sur le cyberespace ont été publiées, afin de sensibiliser et informer les acteurs spécialisés de la Principauté.
**52** « Les essentiels de la cyber » ont été adressés à différentes autorités. Ce document résume, sans élément technique, les faits les plus marquants. Ainsi, les autorités et les hauts responsables peuvent être sensibilisés aux grands événements mondiaux dans le domaine de la cybersécurité.
**25 alertes de sécurité, dont 13 nécessitant une prise en compte immédiate**, ont été émises. Ces documents sont destinés à prévenir les équipes techniques opérationnelles des parties prenantes de l'AMSN, d'un danger imminent sur des logiciels ou équipements informatiques, **↘-45%**.
**1127 avis de sécurité**, documents faisant état de vulnérabilités sur des logiciels ou équipements informatiques et des moyens de s'en prémunir, ont été diffusés afin d'éviter la compromission des systèmes d'information, **↗+13%.**

## DESTRUCTION DES SUPPORTS NUMÉRIQUES ET RECYCLAGE

En 2022, la Société Monégasque d'Assainissement (SMA), a détruit 2906 supports de données numériques (disques, bandes, clés USB, mémoires SSD, etc.), grâce à son offre DataDestruction.

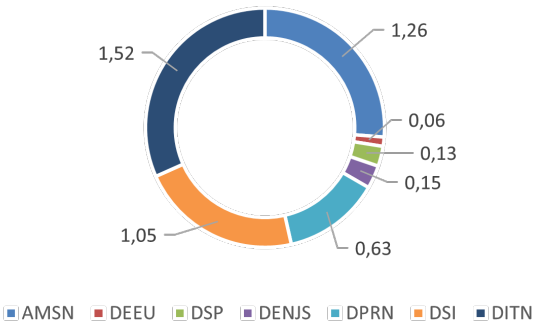
Prestation entièrement réalisée sur le territoire monégasque par un personnel dédié et avec une traçabilité garantie, elle consiste en une destruction physique selon la norme DIN 66399.

Les particules résultantes, totalement inutilisables, suivent ensuite la filière de recyclage des Déchets d'Équipements Électriques et Électroniques (D3E).

# FINANCEMENT DE LA SÉCURITÉ NUMÉRIQUE

La loi n° 1.519 du 23 décembre 2021 portant fixation du budget général primitif de l'exercice 2022, adoptée par le Conseil National dans sa séance du 16 décembre 2021, prévoyait 4,8M€ pour la sécurité numérique à l'article 708.946. Cet article budgétaire, permettant de décliner les objectifs stratégiques prioritaires du Gouvernement en matière de sécurité numérique, regroupe les besoins de tous les services exécutifs de l'État en matière de sécurité numérique ainsi que les participations de l'État dans des opérations de cybersécurité bénéficiant aux entreprises et aux résidents de la Principauté.

**Article 708 946 - budget 2022 par département/direction en M€**




Cet article budgétaire a permis en 2022 les réalisations suivantes :

– L'AMSN a notamment :

- pu prendre en charge l'accompagnement pour l'obtention de la qualification de Prestataire de Service de Confiance de : la Direction de l'Expansion Economique (DEE), la Direction des Ressources Humaines et de la Formation de la Fonction Publique (DRHFFP), la Direction de la Sûreté Publique (DSP), la Direction des Services Numériques (DSN) et la Mairie ;
- continué le déploiement de systèmes de détection d'attaques informatiques au bénéfice de 2 nouveaux OIVs ;
- financé le renouvellement du logiciel Monaco Care Safety pour les internautes de la Principauté ;
- réaménagé son « Security Operation Center » afin de renforcer l'équipe de veille ;
- étendu le réseau de sécurité nationale à 2 nouveaux sites.

– La Délégation Interministérielle chargée de la Transition Numérique (DITN) a continué d'animer la mise en œuvre des analyses de risques et des audits, prévus par la Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E), pour les projets numériques des services exécutifs de l'État. Ainsi, en 2022 :

- 35 systèmes d'information ont été homologués ;
- 12 systèmes d'information ont fait l'objet d'un renouvellement de leur homologation ;
- 9 systèmes d'information ont fait l'objet d'un audit.

– La Direction des Plateformes et des Ressources Numériques (DPRN) a continué la mise en œuvre du chantier majeur de modernisation et de sécurisation du réseau informatique du Gouvernement. 75% des sites des services exécutifs de l'État ont ainsi été migrés sur de nouvelles technologies.

– La Direction des Systèmes d'Information (DSI) a renforcé ses équipes opérationnelles avec 4 consultants en sécurité, a réalisé différents travaux de sécurisation de locaux techniques et a procédé à l'achat de licences de produits de sécurité.

– La Direction de la Sûreté Publique (DSP), la Direction de l'Eduction Nationale, la Jeunesse et des Sports (DENJS) et le Département de l'Equipement de l'Environnement et de l'Urbanisme (DEEU) ont continué de renforcer la mise en conformité à la PSSI-E de leurs systèmes d'information.

# LA STRATÉGIE NATIONALE POUR LA SÉCURITÉ NUMÉRIQUE

## RÉALISATIONS EN 2022

**Protéger les intérêts fondamentaux,** la sécurité des systèmes d'information des institutions officielles de la Principauté et des infrastructures critiques, ainsi que la gestion des crises informatiques majeures :

- La mise en place des mesures règlementaires de sécurité pour les Opérateurs d'Importance Vitale (OIV), débutée en 2018, s'est poursuivie en 2022. Certains secteurs d'activité sont plus avancés que d'autres. Les calendriers d'implémentation des mesures règlementaires ont été revus avec les OIV ; certains ont demandé une modification du calendrier car les chantiers étaient plus complexes qu'initialement prévu. Globalement, la mise en conformité devrait donc aboutir en 2024.
- La protection des établissements, installations ou ouvrages exploités par les OIV a été renforcée et fait l'objet d'un plan particulier de protection qui doit être validé par la Direction de la Sûreté Publique, conformément à l'arrêté ministériel n°2020-902 du 21 décembre 2020. A date, **20 Plans Particuliers de Protection** ont été validés par la Direction de la Sûreté Publique.
- Au 31 décembre 2022, 8 OIV (+2) bénéficient du service de détection des attaques mis en œuvre par l'AMSN et opéré par son entité SOC-MC.
- Le CERT-MC a traité 11 incidents de sécurité (↘**-63%**) à la suite d'attaques par hameçonnage ou d'exploitations de vulnérabilités des systèmes d'information de l'État et des OIV. Le traitement de ces incidents a mobilisé 10 jours homme en 2022.
- **1127** avis de sécurité ont été diffusés en 2022 vers les OIV et les services de l'État. Ce nombre est en augmentation (↗**+13%**). Ces documents font état de vulnérabilités et des moyens de s'en prémunir, afin d'éviter la compromission des systèmes d'information concernés.

**Développer la confiance dans le numérique,** le respect de la vie privée numérique, la protection des données personnelles et l'appréhension de la cyber malveillance :

- **35 systèmes d'information** de l'État ont fait l'objet d'une démarche d'homologation en 2022 afin de s'assurer de leur sécurisation. Par ailleurs, **12 systèmes d'information** ont vu leur homologation renouvelée.
- **9 audits** ont été effectués par des Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI) qualifiés par l'AMSN, afin de vérifier le niveau de sécurité appliqué aux systèmes d'information de l'État.
- Le périmètre de l'Infrastructure de Confiance Nationale, qui permet la délivrance de certificats pour les services électroniques (cachet électronique, signature électronique), a été élargi aux services exécutifs de l'État. La qualification de la Mairie, de la Direction de la Sûreté Publique, de la Direction des Ressources Humaines et de la Formation de la Fonction Publique, de la Direction de l'Expansion Economique et de la Direction des Services Numériques a été prononcée en septembre 2022.
- Monaco Care Safety, service gratuit pour les clients de Monaco Télécom lancé en juillet 2019, offert par le Gouvernement Princier, qui permet d'obtenir 10 licences d'antivirus, de contrôle parental pour la navigation sur Internet et de navigation sécurisée sur Internet, compte **1332** clients actifs au 31 décembre 2022 (↗**+15%**). Malgré la croissance, le nombre de clients ayant activé la solution ne représente que **7,2%** du parc. Un effort de communication et de sensibilisation est programmé en 2023 par Monaco Telecom.

**Développer les sensibilisations et les formations initiales et continues :**

Le personnel de l'AMSN a suivi 20 formations spécialisées en présentiel ou à distance. Ces formations se poursuivront en 2023, en particulier pour les nouveaux recrutements :

- 3 stages au CFSSI[2] sur la sécurité des systèmes d'information et la sécurité des infrastructures virtualisées ;
- 1 exercice pratique de 3 jours pour 5 personnes sur l'investigation post-incident, créé sur la base de scenarios issus d'attaques réelles ;
- 12 formations sur le système de gestion des événements de sécurité Splunk.

**Faire de la sécurité du numérique un facteur de compétitivité :**

- Pour la quatrième année consécutive, les entreprises monégasques étaient représentées aux « Assises de la Sécurité » autour de l'AMSN sous l'enseigne de « Monaco Cyber Security Initiative ». Cette participation permet aux entreprises monégasques de prendre la place qui leur revient dans le monde de la cybersécurité et de démontrer que la Principauté est aujourd'hui un acteur à part entière dans ce domaine. Les Assises ont réuni lors de cette 22ème édition 164 sociétés partenaires, 20 startups, 120 experts et journalistes, et 1350 invités (↗+12%). Parmi ces acteurs monégasques, Monaco Cyber Security Initiative a réuni :

monacotelecom
Smart Global Governance
Lutessa MONACO
MVE
KPMG
pwc
LUXTRUST®
monaco cyber sécurité
Pineappli SO SAFE - SO EASY - SO DIGITAL

- Au 31 décembre 2022, 5 entreprises sont qualifiées « Prestataire d'Audit de la Sécurité des Systèmes d'Information » (PASSI) et 39 auditeurs en sécurité de systèmes d'information ont obtenu leur attestation de compétence pour réaliser des audits en Principauté.

# FOCUS SUR L'INFRASTRUCTURE DE CONFIANCE NATIONALE

Le projet d'Infrastructure de Confiance Nationale (ICN) a débuté en 2019 avec pour vocation de mettre en place une infrastructure à la fois technique et organisationnelle pour permettre aux services publics la délivrance des certificats électroniques à valeur probante.

Ces certificats dits qualifiés au sens de la réglementation monégasque[3] servent de socle au projet d'Identité Numérique piloté par la Direction des Services Numériques.

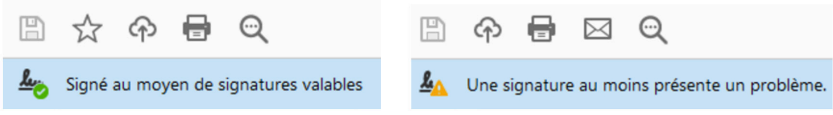
Mise en place et pilotée par l'AMSN[4], l'ICN répond aux plus hauts standards internationaux en matière de sécurité et met en œuvre des mécanismes cryptographiques.

A ce jour, l'ICN a permis la production d'environ 20 000 certificats électroniques au profit :

- des citoyens à travers la Mairie pour l'authentification et la signature électronique,
- des résidents au travers de la Direction de la Sûreté Publique pour l'authentification et la signature électronique,
- des entreprises au travers de la Direction de l'Expansion Economique pour l'authentification, la signature et le cachet électroniques,
- des chefs de services de l'État au travers de la Direction des Ressources Humaines et de la Formation de la Fonction Publique pour l'authentification, le cachet et la signature électroniques,
- des services de l'État au travers de la Direction des Services Numériques pour de l'horodatage électronique.

Après un processus d'audit d'une durée de 10 mois, ces 5 services ont obtenu la qualification de Prestataires de Services de Confiance (PSCo). Pour pérenniser la confiance, ce processus est revu annuellement.

L'AMSN travaille désormais à la rédaction des dossiers de demande de reconnaissance auprès de la société Adobe. Le programme proposé par Adobe s'intitule AATL (Adobe Approved Trust List). Il vise à permettre aux utilisateurs du monde entier de vérifier automatiquement la validité des documents signés électroniquement, dès leur ouverture dans le logiciel Adobe® Acrobat® ou Reader®. Ce programme a le mérite d'éviter la confusion pour l'utilisateur en apportant une indication visuelle sur la présomption de validité de la signature (coche verte en lieu et place de l'avertissement orange).




[3] Arrêté Ministériel n° 2020-461 du 6 juillet 2020 portant application de l'article 13 de l'Ordonnance Souveraine n° 8.099 du 16 juin 2020 fixant les conditions d'application de la loi n° 1.383 du 2 août 2011 pour une Principauté numérique, modifiée, relative aux services de confiance qui constitue le Référentiel Général de Sécurité de la Principauté.
[4] Article 3b) de l'Ordonnance Souveraine n° 8.504 du 18 février 2021 portant application de l'article 24 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique.

# LES SUJETS QUI DEVRONT ÊTRE ADRESSÉS

## DE NOUVELLES ORIENTATIONS LÉGISLATIVES

La contrefaçon informatique et l'absence de protection des droits d'auteur de logiciels sont des sujets qui sont pris en compte dans l'évaluation de l'UIT et qui devront donc être adressés dans le calendrier législatif. Le Gouvernement a déposé le 14 septembre 2021 le projet de loi n°1045 portant reconnaissance et régime de la propriété des œuvres de l'esprit ; ce dernier devrait permettre d'apporter une réponse adéquate.

La modernisation du cadre législatif relatif à la protection des données personnelles est un des chantiers nécessaires. En effet, même si la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée, adresse ce sujet, plusieurs thèmes restent à préciser. Il s'agit notamment de l'absence d'obligation de notification à l'autorité de protection et à la personne concernée, lorsque se produit un incident ou une violation de données. Ce sujet est abordé par le projet de loi n° 1054 déposé auprès du Conseil National le 20 décembre 2021.

La convention de Budapest est amenée à évoluer au travers d'un deuxième protocole additionnel adopté par le Comité des Ministres du Conseil de l'Europe le 17 novembre 2021. Celui-ci prévoit :

- une base juridique pour la divulgation des informations relatives à l'enregistrement des noms de domaines et pour la coopération directe avec les fournisseurs de services pour les informations sur les abonnés ;
- des moyens efficaces pour obtenir des informations sur les abonnés et les données relatives aux échanges numériques ;
- une coopération immédiate en cas d'urgence ;
- des outils d'entraide ;
- des garanties en matière de protection des données à caractère personnel.

Le texte a été ouvert à la signature le 12 mai 2022. Le Gouvernement étudie l'opportunité de ce nouveau protocole.

## DES MESURES TECHNIQUES ET ORGANISATIONNELLES

Un volet cyber devra être formellement intégré aux plans de secours nationaux existants.

Par ailleurs, une coordination nationale cyber devra intégrer les préoccupations techniques permettant un retour à un état de sécurité optimal, tout comme les enjeux stratégiques, qui devront prendre en compte le maintien des activités affectées par la crise.

Des exercices de cybersécurité et de gestion de crise devront être joués régulièrement avec les différentes entités en charge de la sécurité numérique, avec pour objectif une bonne coordination interservices et la mise en place des moyens nécessaires pour faire face à ces crises.

La Stratégie Nationale pour la Sécurité Numérique devra être revue pour prendre en considération l'évolution des risques et intégrer une feuille de route pour sa mise en œuvre.

**Agence Monégasque de Sécurité Numérique**

24 rue du  Gabian
MC 98000 Monaco
Tél : +377 98 98 24 93
www.amsn.gouv.mc

Gouvernement Princier
PRINCIPAUTÉ DE MONACO