AiOc
Ingénierie Midi-Pyrénées

N° SPECIAL RRI
18 & 19 Février 2026

Fédération cinov MIDI-PYRÉNÉES

CYBERSÉCURITÉ : ÉTAT DE LA MENACE ET ÉVOLUTIONS RÈGLEMENTAIRES

Transformer la peur du risque en culture de la protection : Rémy Daudigny, délégué à la sécurité numérique pour l'Occitanie au sein de l'Agence nationale de la sécurité des systèmes d'information (Anssi), fait le point sur l'état de la menace et les nouvelles directives européennes qui vont s'appliquer en France.

RÉMY DAUDIGNY

La cybersécurité : une définition

Défendre, connaître, partager, accompagner, réguler : les cinq missions de l'Anssi définies par Rémy Daudigny en introduction de son propos disent les niveaux d'actions menées au plan national pour se défendre face à la menace. Une menace que l'on peut contrer dès lors qu'on l'a prise en compte et qu'on l'a clairement identifiée. « La cybersécurité, c'est l'action de se mettre en sécurité par rapport à la menace cyber. On ne peut plus mésestimer ce risque numérique qui pèse sur toutes les activités. Aujourd'hui, la cybersécurité s'appuie sur trois piliers : une dimension technophile bien entendu, un cadre juridique adéquat et une organisation susceptible de faire vivre ces systèmes d'information. »

La menace cyber : une réalité

« La menace cyber présente deux grandes facettes : une menace stratégique et historique qui est liée à l'espionnage (visant les décideurs politiques, les grands donneurs d'ordre, espionnage économique sur nos entreprises.) Et une menace systémique, qui vous concerne, opérée par des acteurs criminels, des groupes particulièrement organisés, qui vendent leurs services au plus offrant, qui ont développé des logiciels, des activités mécanisées, des franchises, et dont le but est l'extorsion de fonds. Aujourd'hui, on n'a pas besoin d'être une cible pour être une victime. » Avec une frontière entre menace stratégique et menace systémique qui tend à être de plus en plus poreuse. « L'État protège les intérêts fondamentaux de la nation, met en place des dispositifs d'accompagnement, mais c'est à chaque citoyen, à chaque chef d'entreprise, de faire sa part, et de se mettre en sécurité par rapport à cette menace. Dans cet espace conflictuel actuel, où d'aucuns nous promettent un conflit hybride de haute intensité sur le sol européen avant 2030, chacun est responsable de la sécurité des autres. »

La réponse européenne : NIS2

Après avoir accompagné 1 000 entités publiques, dont 700 collectivités territoriales, dans le cadre de France Relance, dans le durcissement de leur système d'information, l'Anssi anticipe la mise en conformité à la directive européenne NIS2, pensée pour contrer la sophistication croissante des attaques. Ce texte européen s'applique à tous les États membres et a pour mission d'élever de manière significative le niveau de cybersécurité du secteur économique. « NIS2 va concerner les entreprises en fonction de leur taille et de leur secteur d'activité explique Rémy Daudigny, et demande de répondre à trois grandes obligations : l'enregistrement, la gestion des risques et la déclaration d'incidents. Le pire réflexe, c'est l'inaction. »

Les ressources

- **Messervicescyber :** cette plateforme numérique de l'Anssi propose un diagnostic cyber gratuit.
- **MonEspaceNIS2 :** information, test et préenregistrement.

SOMMAIRE

aioc actu est une publication de l'AiOc
(Immeuble Belvédère 11 bd des Récollets
31078 Toulouse cedex)

Directeurs de publication :
David PASIN
et Damien DUTHEIL

Coordination éditoriale :
Lucy Haas

Conception / Réalisation :
Ligne Sud

Illustration :
Hélène RESSAYRES et Rémy GABALDA

RENCONTRES RÉGIONALES DE L'INGÉNIERIE
INAUGURATION 2026

David PASIN et Damien DUTHEIL

David Pasin,
Président AIOC
« La cybersécurité, thème central de ces deux jours de Rencontres, peut sembler, à première vue, éloignée de nos activités quotidiennes. Pourtant, elle s'impose désormais comme une dimension incontournable, tant dans notre sphère professionnelle que personnelle, et vient enrichir les enjeux traditionnels de sûreté. Ces Rencontres régionales de l'ingénierie, évènement unique en son genre en France, sont aussi l'occasion de valoriser l'expertise de l'Occitanie : un jury y distingue des partenaires, des adhérents et des étudiants pour leurs projets innovants, illustrant ainsi la diversité et la richesse de nos engagements. »

Damien Dutheil,
Président de la Fédération Cinov Midi-Pyrénées
« Le thème qui nous rassemble cette année, portant sur la sûreté et la cybersécurité dans l'acte de construire, illustre parfaitement notre capacité à échanger, à partager des innovations, des idées. Chaque défi technologique a été un levier d'optimisation, d'innovation. Chaque nouvelle exigence a constitué une invitation à progresser et chaque risque identifié est une chance d'améliorer nos pratiques. Intégrer la sûreté et la cybersécurité dans notre réflexion, c'est anticiper plutôt que subir, mais c'est surtout protéger les usagers de nos bâtiments et leur offrir une sérénité au quotidien. »

Dominique Lagarde,
Vice-Président du Sicoval
« C'est avec un grand plaisir que nous accueillons sur le territoire du Sicoval cette 17e édition des Rencontres régionales de l'ingénierie. Un territoire qui incarne l'audace et l'innovation, deux valeurs qui résonnent particulièrement avec le thème que vous avez choisi cette année, sûreté et cybersécurité dans l'acte de construire. En effet la cybersécurité est désormais un pilier de la confiance, de la fiabilité, une démarche impérative. Les défis sont immenses : la montée des cybermenaces, la complexité des infrastructures, l'enjeu de souveraineté. Mais les solutions existent et elles naîtront de notre capacité à travailler main dans la main, élus, ingénieurs, entreprises et citoyens. »

Michel Colombié,
représentant de la CCI Occitanie
« La cybersécurité est devenue une réalité opérationnelle qui transforme profondément nos industries et nos pratiques. À l'heure où l'intelligence artificielle se développe à grande vitesse, suscitant à la fois enthousiasme et vigilance, nous devons collectivement repenser nos méthodes. Dans ce contexte, les chambres de commerce et d'industrie jouent un rôle essentiel, en accompagnant les entreprises, et notamment les petites structures, pour leur permettre d'adopter de bonnes pratiques et renforcer leur niveau de protection. Les Rencontres 2026 constituent une plateforme idéale pour échanger, partager nos expériences et imaginer l'ensemble, l'avenir de notre secteur. »

Laurent Chérubin,
conseiller régional de la Région Occitanie
« Plus que jamais, il faut monter en compétence sur ces sujets de cybersécurité que vous allez évoquer durant ces deux jours de Rencontres, prendre en considération les risques qui sont les nôtres, les risques qui vont se poser à l'avenir. Et se protéger. Tous ces enjeux-là, la Région Occitanie les a pris en considération, les a anticipés en créant Cyber'Occ, qui a vocation à accompagner, à aider les collectivités, les territoires, les entreprises, pour conserver notre savoir-faire et notre ambition locale. »

Ingénierie Midi-Pyrénées

COMMENT DÉCELER UNE CYBERATTAQUE ET COMMENT S'EN PRÉMUNIR ?

Comment déceler les signes d'une attaque ? Comment mettre en place des moyens de prévention face à des assauts de plus en plus sophistiqués et innovants ? Comment se prémunir, collectivement face aux menaces croissantes d'un monde de plus en plus connecté ? Éléments de réponse.

...

La cible

La priorité avant de déterminer un plan d'actions, est de définir avec précision ce que l'on souhaite protéger, et établir un état des lieux des mesures de protection mises en place. « Ce qui nous préoccupe avant tout lorsque nous accompagnons des organisations dans leurs diagnostics de maturité cyber, explique Caroline de Rubiana, c'est la donnée : où est-elle est, qui y a accès, à qui peut-on la confier ? La donnée, c'est la ressource à protéger, c'est donc le point de départ de tout questionnement lié à la cyber ». Un état des lieux primordial, à la base de tout questionnement, comme le confirme Olivier Nisse, du Ministère des Armées : « Notre action est tournée vers les entreprises qui souhaitent contractualiser avec le Ministère des Armées. Lorsque l'entreprise rejoint ce cercle-là, notre première réaction est effectivement d'évaluer sa maturité cyber. Quelle est l'organisation en place ? Quelle est la facilité d'accès au système d'information, techniquement, physiquement ? Le temps de la sensibilisation vient dans un deuxième temps, puis le conseil dans la sécurisation du système d'information en fonction de la sensibilité des données que nous allons confier à l'entreprise. »

La faille

Caroline de Rubiana, responsable Csirt Occitanie, Cyber'Occ : « Ce qu'ont bien compris les attaquants, comme tous les escrocs du monde, c'est qu'on peut manipuler l'humain. Bien plus qu'une machine. Donc, les cyberattaques commencent à 80 % par un simple mail. Souvent envoyé un vendredi soir, ce qui laisse tout le week-end au virus ou à l'attaque de se déployer tranquillement. » L'humain, voilà donc la faille, également identifiée par Olivier Nisse, expert en cybersécurité : « Nous sommes confrontés à des points d'attaque finalement très bas de gamme. La clé USB infectée. Le QR code qui redirige vers une cyberattaque. C'est le niveau zéro de la cybersécurité. » Mais suffisant pour infiltrer un système et mettre en péril la sécurité d'une entreprise. « Aujourd'hui, nous connaissons des menaces qui passent par nos partenaires pour nous atteindre, explique Véronique Bardet, des Laboratoires Fabre. Nos cabinets d'avocats, de notaires, qui disposent dans leurs boites mails de tous nos contacts. C'est cette boite qui va d'abord être attaquée, parce qu'elle est moins surveillée, pour nous atteindre. » Guillaume Jicquel : « Mettre des millions sur un point de vigilance si le prestataire, l'avocat, a accès à notre messagerie, à nos informations, à nos documents, ça ne sert à rien. La majorité des incidents n'ont pas lieu sur ce que l'on souhaite protéger au maximum. La source est à côté, on ne l'a pas protégée, et elle va avoir un impact chez nous. »

Le rempart

Premier rempart clairement exposé : la prise de conscience, la sensibilisation. Puisque l'humain est la porte d'entrée, il faut qu'il soit conscient des dangers. Caroline de Rubiana : « On ne peut pas se sécuriser du jour au lendemain. Mais si on a mis en place une sensibilisation, une information, si on a défini un référent cybersécurité à qui on peut s'adresser en cas de doute par exemple, on peut réagir. » Un réflexe également prôné par Guillaume Jicquel : « Le fait d'avoir clairement désigné un référent permet de communiquer avec les services, les équipes, les managers, la partie RH, pour acculturer, alerter sur des comportements à risque. » La >

Avec la participation de :

- **Caroline de Rubiana,** responsable Csirt Occitanie, Cyber'Occ.
- **Véronique Bardet,** directrice IT cyber-sécurité, Laboratoires Pierre Fabre.
- **Denis Boudy,** consultant stratégie digitale et cyber-sécurité.
- **Olivier Nisse,** expert en cyber-sécurité spécialisé Défense en Région Occitanie, Ministère des Armées.
- **Guillaume Jicquel,** Ingénieur, représentant l'AiOc et la Fédération Cinov Midi-Pyrénées.

> « Ce qu'ont bien compris les attaquants, comme tous les escrocs du monde, c'est qu'on peut manipuler l'humain. Bien plus qu'une machine.»

sensibilisation, régulière, la formation, c'est également le rempart constitué par les équipes de Véronique Bardet, en complément des pares-feux techniques. « Nous travaillons régulièrement à la vigilance de nos collaborateurs. Il y a quatre ans, nous avons subi une interruption totale de notre activité, après une attaque qui s'est propagée au travers d'un mail dans une filiale en Italie. Nous savons maintenant qu'agir, de façon efficace, peut se faire à tout niveau. Changer son mot de passe, imposer un double regard dès qu'on a un doute, un double facteur d'authentification. Ce sont des choses simples, qui fonctionnent dès lors qu'on est sensibilisés à la menace. Nous menons également des campagnes d'information, de formation, et de tests auprès de nos collaborateurs. Lors de nos journées de formation sur la sécurité, on ajoute une partie sur la cyber. » Denis Boudy : « Nous devons, tous ensemble, acquérir cette compétence, être conscience de toutes les conséquences quand on manipule de la donnée, quand on crée de la donnée. Ne laissons pas nos documents numériques n'importe où, vérifions si la porte est bien fermée à clé et à qui on laisse les clés. »

La réaction

Le cloisonnement peut être une forme de réponse pour se prémunir d'une attaque de grande ampleur, comme le souligne Véronique Bardet : « On ne pourra pas prévenir toutes les attaques, qui sont quotidiennes. Par contre on peut réagir plus vite parce qu'on va la reconnaître et circonscrire son impact avec des cloisons virtuelles, entre nos lignes de production par exemple. » Guillaume Jicquel : « Le risque zéro n'existera jamais. Il faut penser la cyber comme une plus-value à apporter face à la concurrence et minimiser l'impact de l'attaque sur nos organisations en ayant au préalable pensé nos systèmes d'information. » Comme Denis Boudy, tous prônent l'anticipation : « Se préparer à vivre une cyberattaque est primordial, cela permet de mieux réagir lorsque cela arrive. »

Denis Boudy


Caroline de Rubiana


Véronique Bardet


Guillaume Jicquel


Olivier Nisse

Ingénierie Midi-Pyrénées

COMMENT ASSURER LA SÛRETÉ DES BÂTIMENTS ET LEURS FONCTIONNALITÉS ?

Assurer la sûreté des bâtiments tout en préservant leurs fonctionnalités : un enjeu complexe qui implique dès l'expression du besoin, de combiner prévention, technologie maîtrisée et gestion des risques.

...

Le nouveau visage de la menace

Au rang des menaces auxquelles les entreprises françaises doivent faire face, la menace cyber ne doit pas à elle seule éclipser les problématiques de sécurité qui impactent toujours les bâtiments, la protection des personnels, et l'ensemble des dispositifs qui permettent de se protéger d'actes malveillants. Bruno Magicato, chargé de mission pilotage des évolutions des infrastructures pour le CNES, le souligne d'emblée : « Il semble aujourd'hui plus facile d'être attaqué et pénétré par tout ce qui est attaque cyber que par des attaques physiques. Il n'empêche qu'il convient de se protéger physiquement, et pas seulement au niveau des réseaux, contre des actes malveillants. Et dans la mesure où les systèmes de sécurité sont eux-mêmes connectés, une prise en compte globale de la menace est indispensable. » D'autant plus, si comme l'explique Gilles Laborde, la menace est hybride : « La désinformation, la manipulation, des infiltrations, des provocations viennent mettre en péril nos intérêts. Demain, des menaces physiques, avec des drones, des lasers, qui peuvent être des outils d'attaque, des systèmes à génération de champs électromagnétiques, voire d'impulsions électromagnétiques. Il va falloir y réfléchir par anticipation, on y va tout droit dès demain. »

L'état de la menace

« L'urgence, c'est d'analyser le besoin, de définir contre quoi on veut se protéger, explique Bruno Magicato. À partir de là, on peut définir des systèmes de protection, une protection progressive et bien ciblée, du simple contrôle d'accès visuel au système de badge, jusqu'à de l'identification plus sévère au cœur du système. Il faut connaître la menace pour mettre en place le bon système qui va assurer la bonne protection contre le risque réel. » Exemple chez Safran où la menace est multiple, comme l'explique Vincent Vidal. « Nous mêlons activité aéronautique, civile, militaire, activité défense, spatiale, optique. Cette diversité génère forcément des menaces multiples, endogènes ou exogènes. Les bâtiments en eux-mêmes, même dans le cadre d'une activité identique, divergent : bâtiments de production, tertiaires, labos de recherche, datacenters. Cette diversité est à prendre en compte dans l'évaluation de la menace. Aujourd'hui, il n'y a plus de petit système. La moindre ampoule connectée peut-être une porte d'accès à votre Wi-Fi. » Mais la menace n'a de sens que si on a clairement défini ce qui était menacé, comme l'énonce Patrice Merle : « Pour chaque type d'établissement, nucléaire, militaire, aéronautique, bâtiments publics, de la mairie à l'école, la menace est différente. Notre réponse ne peut passer que par du sur-mesure si on veut qu'elle soit efficace. »

Security by design

Vincent Vidal : « Avant même le premier coup de crayon, nous menons une vraie analyse de la menace et de nos biens à protéger. Dans un deuxième temps nous passons à ce qu'on appelle le Security by Design : concevoir le bâtiment en fonction de l'usage, mais aussi en fonction de la sûreté et de son environnement.

>

Avec la participation de :

- **Gilles Laborde,** président, Cluster Primus.
- **Vincent Vidal,** responsable sûreté sites, Safran.
- **Michel Bernado,** expert en sûreté Défense, ministère des Armées.
- **Bruno Magicato,** chargé de mission pilotage des évolutions des infrastructures, CNES Toulouse.
- **Patrice Merle,** ingénieur, représentant AIOC et fédération Cinov-Midi-Pyrénées.

« L'urgence, c'est d'analyser le besoin, de définir contre quoi on veut se protéger, »

Aujourd'hui, la sûreté n'est plus un lot que l'on ajoute en fin de construction, c'est un lot transverse qu'on aborde dès l'expression du besoin. » Patrice Merle : « On va chercher l'usage, on va comprendre la menace, le risque, pour le décliner en ingénierie, en cahier des charges, de façon plus précise. Pour être sûr de répondre au fonctionnel, mais surtout aux moyens du maître d'ouvrage, en termes d'exploitation, de maintenance, de gardiennage, et mettre ainsi en place un outil qui répondra vraiment aux besoins, et sera exploitable et maintenable ». Michel Bernado : « Que cette phase se situe le plus en amont possible, ça sera, en termes de design, intéressant, mais également en termes de coût. Une fois que le bâtiment est construit, il est difficile de venir ajouter des éléments de détection, de volumétrie, de vidéo. »

Sensibilisation

Pour Gilles Laborde, le premier sujet fondamental à appréhender dans ce cadre demeure le risque du facteur humain, « qu'on va essayer d'amortir avec de la sensibilisation, de l'information, des exercices, de façon à ce que chacun prenne conscience du risque qu'il prend, des menaces très concrètes. Il faut passer du stade de la naïveté à celui d'experts, à un éveil permanent. Et il faut traiter cet aspect sécurité, sûreté, comme on fait de la prévention dans le domaine des accidents de travail. Il faut que ça se devienne une culture. Il est essentiel que tout le monde adhère à cette culture. » Une idée partagée par Michel Bernado : « Le tout numérique, le tout technologique n'est pas une solution. L'ensemble des mesures, d'organisation, de sensibilisation, de protection physique et bien sûr, des mesures techniques doit être envisagé. »

« Ce qui me semble particulièrement important sur l'efficacité de tous les dispositifs de sûreté qu'on peut mettre en place, c'est leur acceptabilité, pointe Vincent Vidal. Si les mesures de sûreté que l'on met en place sont mal acceptées, incomprises, forcément, la nature humaine étant ce qu'elle est, il y aura des gens qui vont essayer de passer outre, parfois pour de très bonnes raisons. Et donc, si ces mesures de sûreté ne sont pas acceptées, elles seront forcément dévoyées. »

> « On va chercher l'usage, on va comprendre la menace et le risque, pour le décliner en ingénierie »

(de gauche à droite) Vincent Vidal, Michel Bernado, Bruno Magicato et Gilles Laborde.

PRIX RÉGIONAL
19 FÉVRIER 2026

Ingénierie Midi-Pyrénées

PRIX DES RENCONTRES RÉGIONALES DE L'INGÉNIERIE 2026

Le Prix des Rencontres régionales de l'ingénierie récompense des projets, produits ou méthodes innovants intégrant les trois composantes du développement durable : environnementale, sociale et économique.

Les lauréats

Catégorie Bureaux d'ingénierie membres de l'AIOC et de la fédération CINOV Midi-Pyrénées

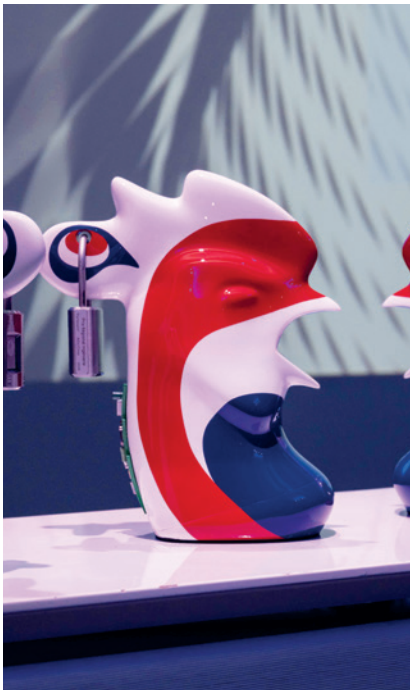
GAXIEU
pour la réutilisation des eaux usées de la station d'Argelès-sur-Mer pour de l'irrigation agricole

Catégorie Etudiants

INSA
pour l'analyse du comportement structurel des réseaux de poutres bidirectionnels dans la construction de bâtiment

Catégorie Partenaires industriels

SOLSTYCE
pour la valorisation photovoltaïque par ombrieres sur route departementale



Les lauréats de l'édition 2026 ont remporté un Coq (ci-contre), oeuvre de l'artiste Cédric Soulette. Le prix étudiant était doté de 500 €.

LES PARTENAIRES
2026
...

ATLANTIC
www.atlantic.fr

BOURDARIOS
france.vinci-construction.com/fr

BUESA
buesa.com

CID GROUPE CLIMATER
www.groupe-climater.com/cid

CLARAC ESPACES VERTS
clarac-espacesverts.com

CLIVET
www.clivetfrance.fr

COLAS
www.colas.com/fr

DALKIA
www.dalkia.fr

DEMATHIEU BARD
www.demathieu-bard.fr

ECOFOREST
ecoforest.com/fr/

EIFFAGE CONSTRUCTION
www.eiffageconstruction.com

EIFFAGE ENERGIE SYSTEMES
www.eiffageenergiesystemes.com

EIFFAGE INFRASTRUCTURES
www.eiffagegeniecivil.com

ENGIE SOLUTIONS
www.engie-solutions.com/fr

EQUANS
www.equans.fr

EUROVIA MIDI-PYRENEES
www.eurovia.fr

FAUCHE
www.fauche.com

FONDERIES DECHAUMONT SA
www.fonderies-dechaumont.com

GROUPE GB
groupe-gb.fr

GHM - ECLATEC
www.ghm-eclatec.com

GRUNDFOS
www.grundfos.com/fr

ID VERDE TOULOUSE CREATION
idverde.fr/

EQUANS
www.equans.fr/

JOHNSON CONTROLS HITACHI
www.hitachiclimat.fr/

KNAUF INSULATION
knauf.com/fr-FR/knauf-insulation

LACROIX
www.lacroix-environment.fr/

LAFARGE
www.lafarge.fr

LEGENDRE OCCITANIE
www.groupe-legendre.com/

MAF
www.maf.fr

MAPEI
www.mapei.com/fr/fr-fr/page-d-accueil

MONTMIRAIL
montmirail.fr

NGE
www.nge.fr

OCCIREP
occirep.com

OPQIBI
www.opqibi.com

PARERA
www.parera.fr

PEINTURES MAESTRIA
www.maestria.fr

PROVILLE
www.proville-urbain.com

RAZEL-BEC
www.razel-bec.com

SAINT GOBAIN PAM
www.pamline.fr

SAINT-GOBAIN SAGEGLASS
www.sageglass.com/fr

SEAC
www.seac-gf.fr

SIEMENS
www.siemens.com

SNEF
www.snef.fr

SOLS MIDI-PYRENEES
sols.fr/nos-agences/sols-midi-pyrenees

SOLSTYCE
www.solstyce.fr

SOPREMA
www.soprema.fr

SPIE
www.spie.com/fr

SPIE BATIGNOLLES
www.spiebatignolles.fr

TECHNAL
www.technal.com

TRANE
trane.eu/fr

URETEK
www.uretek.fr

VERDONE
www.verdone.fr

VINCI CONSTRUCTION
vinci-construction.com/fr

VINCI ENERGIES
www.vinci-energies.com

WILO
wilo.com/fr/fr

L'AIOC ET CINOV OCCITANIE ADRESSENT LEURS PLUS VIFS REMERCIEMENTS :

- **A nos partenaires** qui partagent leurs savoir-faire
- **A nos intervenants et élus** dont l'expertise a su capter l'attention de l'auditoire.
- **A l'agence AWR, Ligne Sud et ToulEco** pour leur professionnalisme ainsi que leur bonne humeur
- **A l'agence A PROPOS** qui a su nous accompagner étroitement et avec efficacité !
- **Cédric Soulette,** l'artiste aux multiples talents qui réalise chaque année des œuvres originales pour nos lauréats.
- Enfin **merci** à tous ceux qui permettent la tenue de cet évènement et dont les interventions se font en backstage !

Secrétariat AiOc – lundi au vendredi de 14h à 18h / Tél. : 06 47 05 16 97 – A Propos / Tél. : 05 62 26 62 42