

Số: /KH-UBND

Hung Yên, ngày tháng 4 năm 2026

## KẾ HOẠCH

### Triển khai thực hiện Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia”

Thực hiện Quyết định số 515/QĐ-TTg ngày 30 tháng 3 năm 2026 của Thủ tướng Chính phủ phê duyệt Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia”; Ủy ban nhân dân tỉnh ban hành Kế hoạch triển khai thực hiện Đề án trên địa bàn tỉnh Hưng Yên, như sau:

#### I. MỤC ĐÍCH, YÊU CẦU

##### 1. Mục đích

- Nâng cao năng lực tổng thể, xây dựng lực lượng bảo vệ an ninh mạng tinh nhuệ, hiện đại, đáp ứng yêu cầu quản lý, bảo vệ không gian mạng trong bối cảnh các công nghệ mới phát triển nhanh chóng.

- Nhằm chủ động phòng ngừa, sẵn sàng ứng phó hiệu quả với mọi nguy cơ, thách thức trên không gian mạng, từ đó bảo vệ vững chắc an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của các tổ chức, cá nhân.

##### 2. Yêu cầu

- Xác định an ninh mạng là trọng tâm của quá trình chuyển đổi số, là nhiệm vụ trọng yếu, thường xuyên, lâu dài và gắn liền với sự phát triển kinh tế - xã hội bền vững.

- Tăng cường năng lực phải đi theo hướng cách mạng, chính quy, tinh nhuệ và hiện đại, đồng thời phối hợp đồng bộ, thống nhất, hiệu quả giữa các lực lượng, xây dựng thể trận an ninh nhân dân trên không gian mạng, huy động sức mạnh tổng hợp của cả hệ thống chính trị và toàn dân trong bảo vệ chủ quyền quốc gia trên không gian mạng.

- Nâng cao năng lực theo hướng toàn diện, tự chủ, tự lực, tự cường, phát triển nguồn nhân lực chất lượng cao, nâng cấp cơ sở vật chất, làm chủ công nghệ và hoàn thiện chính sách để đảm bảo lực lượng luôn sẵn sàng, chủ động ứng phó từ sớm, từ xa, chủ động.

- Tích cực hội nhập quốc tế sâu rộng trong lĩnh vực an ninh mạng trên cơ sở giữ vững độc lập, tự chủ, bảo đảm cao nhất chủ quyền, lợi ích và an ninh quốc gia.

#### II. MỤC TIÊU

##### 1. Mục tiêu chung

Nâng cao năng lực tổng thể, xây dựng lực lượng bảo vệ an ninh mạng tinh nhuệ, hiện đại, nhằm chủ động phòng ngừa, sẵn sàng ứng phó hiệu quả với mọi nguy

cơ, thách thức trên không gian mạng, bảo vệ vững chắc an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

## **2. Mục tiêu cụ thể**

### **a) Đến năm 2030**

- 100% lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại cơ quan, đơn vị trên địa bàn tỉnh quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia, cán bộ trực tiếp quản trị, vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5 phải có chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng do cơ quan có thẩm quyền cấp.

- Thiết lập cơ chế chia sẻ thông tin cảnh báo, điều phối ứng phó sự cố giữa các lực lượng bảo vệ an ninh mạng và các doanh nghiệp an ninh mạng để nâng cao năng lực phòng thủ.

- Phân đầu đạt tỷ lệ tối thiểu 70% các cơ quan, đơn vị trực thuộc UBND tỉnh triển khai, sử dụng các sản phẩm, giải pháp công nghệ chiến lược “Make in Vietnam”. 100% các sản phẩm, dịch vụ an ninh mạng phải được kiểm định, đánh giá trước khi đưa vào sử dụng.

- 100% các hệ thống thông tin sử dụng vốn ngân sách nhà nước được triển khai đầy đủ các phương án bảo đảm an ninh mạng theo cấp độ.

### **b) Tầm nhìn đến năm 2045**

Xây dựng lực lượng bảo vệ an ninh mạng tỉnh Hưng Yên chính quy, tinh nhuệ, hiện đại; góp phần cùng cả nước đưa Việt Nam trở thành quốc gia dẫn đầu khu vực về an ninh mạng. Nâng cao năng lực phòng thủ, chủ động tấn công trấn áp tội phạm mạng và các thế lực thù địch trong mọi tình huống; bảo vệ vững chắc chủ quyền số và an toàn thông tin tại địa phương. Đảm bảo môi trường mạng an toàn, tin cậy cho mọi hoạt động của các cơ quan Đảng, Nhà nước, doanh nghiệp và người dân trên địa bàn tỉnh, phục vụ đắc lực cho sự nghiệp phát triển kinh tế - xã hội bền vững của tỉnh.

## **III. NHIỆM VỤ, GIẢI PHÁP**

### **1. Hoàn thiện thể chế, xây dựng và triển khai các cơ chế, chính sách đặc thù**

- Rà soát, cập nhật, hoàn thiện các văn bản quy phạm pháp luật, văn bản hướng dẫn công tác bảo đảm an ninh mạng bảo đảm đồng bộ, thống nhất, hiệu quả giữa các lực lượng, đáp ứng yêu cầu quản lý, bảo vệ không gian mạng trong tình hình mới.

- Xây dựng khung quản lý rủi ro an ninh mạng của tỉnh trên cơ sở khung quản lý rủi ro an ninh mạng quốc gia, nhằm nâng cao tính chủ động của các cơ quan, tổ chức trong việc phân bổ nguồn lực và giảm thiểu thiệt hại do các cuộc tấn công mạng gây ra.

- Nghiên cứu, hoàn thiện, tổ chức triển khai có hiệu quả cơ chế, chính sách ưu đãi nhằm thu hút, trọng dụng, bồi dưỡng, nâng cao chất lượng nguồn nhân lực cho lực lượng bảo vệ an ninh mạng tỉnh.

## **2. Tổ chức lực lượng an ninh mạng**

- Củng cố, kiện toàn Tiểu Ban An ninh mạng tỉnh.
- Tổ chức xây dựng lực lượng trực tiếp bảo vệ an ninh mạng tại các cơ quan, tổ chức quản lý hệ thống thông tin quan trọng về an ninh quốc gia trên địa bàn tỉnh; bảo đảm đủ năng lực, sẵn sàng bảo vệ, vận hành an toàn các hệ thống thông tin thuộc phạm vi quản lý.
- Tham gia hoàn thiện các cơ chế trao đổi, chia sẻ thông tin, đồng thời xây dựng quy trình phối hợp xử lý chặt chẽ giữa các ban, bộ, ngành, địa phương với nhau và giữa các cơ quan, tổ chức với người dân trong công tác bảo vệ an ninh mạng và ứng cứu sự cố an ninh mạng

## **3. Đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao**

- Hàng năm, tổ chức các khóa đào tạo, tập huấn (trực tiếp hoặc trực tuyến) dựa trên việc khảo sát nhu cầu thực tiễn để cập nhật kiến thức, huấn luyện kỹ năng an ninh mạng cho đội ngũ lãnh đạo quản lý, cán bộ công chức, viên chức và người lao động.
- Cử đi huấn luyện, đào tạo kỹ năng chuyên sâu cho lực lượng chuyên trách bảo vệ an ninh mạng tỉnh theo khung chương trình, yêu cầu kỹ năng do Bộ Công an ban hành, các chương trình đào tạo chứng chỉ quốc tế.
- Tham gia các chương trình diễn tập cấp quốc gia, chương trình diễn tập theo vùng nhằm nâng cao năng lực ứng phó và phối hợp tác chiến mạng.
- Phổ biến, nâng cao kiến thức an ninh mạng cho người dân qua các nền tảng học tập số, “Bình dân học vụ số”, các khóa học đại chúng mở (MOOC) và các chiến dịch truyền thông đại chúng hàng năm.
- Ưu tiên bố trí nguồn lực, bao gồm nhân lực, kinh phí và các điều kiện cần thiết khác, nhằm bảo đảm triển khai hiệu quả công tác đào tạo, phát triển nguồn nhân lực phục vụ hoạt động bảo vệ an ninh mạng trên địa bàn tỉnh.

## **4. Giám sát, chia sẻ thông tin, đánh giá năng lực an ninh mạng**

- Tổ chức nghiên cứu, góp ý và chuẩn bị các điều kiện cần thiết để triển khai Bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng đối với cơ quan, tổ chức, doanh nghiệp khi được ban hành.
- Phối hợp xây dựng nền tảng giám sát, điều hành an ninh mạng quốc gia, thường xuyên báo cáo, thông kê và cập nhật dữ liệu an ninh mạng trên phạm vi toàn quốc, với yêu cầu đảm bảo dữ liệu phải "*đúng, đủ, sạch, sống, dùng chung, thống nhất*".
- Phối hợp xây dựng hệ thống chia sẻ thông tin tình báo an ninh mạng (Threat Intelligence). Mục tiêu là hướng tới hình thành các trung tâm phân tích và chia sẻ thông tin (ISAC) cho các lĩnh vực trọng yếu, nhằm thúc đẩy việc chia sẻ thông tin về các mối đe dọa, lỗ hổng bảo mật và các cuộc tấn công giữa khu vực công và tư nhân.

## **5. Nguồn lực bảo đảm thực hiện**

Nguồn ngân sách nhà nước; nguồn của các doanh nghiệp, tổ chức để triển khai các hoạt động nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng tại địa phương; các nguồn hợp pháp khác theo quy định.

### **IV. TỔ CHỨC THỰC HIỆN**

#### **1. Công an tỉnh**

- Là cơ quan đầu mối, chủ trì tham mưu Ủy ban nhân dân tỉnh tổ chức triển khai thực hiện Kế hoạch; chủ động nghiên cứu, đề xuất các giải pháp, nội dung trọng tâm, bảo đảm việc triển khai đồng bộ, thống nhất và hiệu quả trên toàn địa bàn tỉnh. Tổ chức hướng dẫn, kiểm tra, đôn đốc các sở, ban, ngành, địa phương và các cơ quan, đơn vị liên quan trong quá trình thực hiện; kịp thời phát hiện khó khăn, vướng mắc để tham mưu UBND tỉnh chỉ đạo xử lý. Thực hiện tổng hợp tình hình, kết quả triển khai; định kỳ hoặc đột xuất báo cáo UBND tỉnh và các cơ quan có thẩm quyền theo quy định.

- Chủ trì, phối hợp với các sở, ban, ngành và địa phương tổ chức rà soát, đánh giá hiện trạng công tác bảo đảm an ninh mạng; trên cơ sở đó tham mưu, đề xuất các nhiệm vụ, giải pháp cụ thể nhằm nâng cao năng lực bảo vệ an ninh mạng trên địa bàn tỉnh, phù hợp với yêu cầu thực tiễn và định hướng của Trung ương.

- Triển khai các giải pháp giám sát an ninh mạng, thu thập, phân tích, chia sẻ thông tin, cảnh báo sớm các nguy cơ, sự cố an ninh mạng; đồng thời tổ chức đánh giá năng lực bảo đảm an ninh mạng đối với các cơ quan, tổ chức, doanh nghiệp trên địa bàn theo hướng dẫn của cơ quan có thẩm quyền.

- Xây dựng, củng cố và phát triển lực lượng bảo vệ an ninh mạng tại địa phương theo hướng chuyên trách, tinh nhuệ, hiện đại; tổ chức đào tạo, bồi dưỡng, tập huấn, diễn tập nhằm nâng cao trình độ chuyên môn, kỹ năng nghiệp vụ và năng lực ứng phó, xử lý sự cố an ninh mạng, bảo đảm sẵn sàng đáp ứng yêu cầu trong mọi tình huống.

#### **2. Sở Khoa học và Công nghệ**

- Phối hợp với các cơ quan, đơn vị liên quan triển khai các giải pháp bảo đảm an toàn thông tin, góp phần phát triển hạ tầng số của tỉnh theo hướng an toàn, tin cậy, bền vững; lồng ghép yêu cầu bảo đảm an ninh mạng trong các chương trình, nhiệm vụ khoa học và công nghệ trên địa bàn.

- Tham mưu Ủy ban nhân dân tỉnh thúc đẩy nghiên cứu, phát triển, ứng dụng và ưu tiên sử dụng các sản phẩm, giải pháp an ninh mạng “Make in Vietnam”; đồng thời tăng cường hỗ trợ doanh nghiệp đổi mới sáng tạo, làm chủ công nghệ, phát triển các sản phẩm, dịch vụ an ninh mạng trong nước, từng bước nâng cao năng lực tự chủ về công nghệ.

- Chủ trì, phối hợp thúc đẩy hoạt động nghiên cứu, ứng dụng, chuyển giao công nghệ trong lĩnh vực an ninh mạng; kết nối hệ sinh thái đổi mới sáng tạo, hỗ trợ các tổ chức, doanh nghiệp tham gia các chương trình, đề tài, dự án khoa học và công nghệ liên quan đến an ninh mạng.

### **3. Sở Giáo dục và Đào tạo**

- Chủ trì, phối hợp với các cơ quan, đơn vị liên quan tổ chức lồng ghép nội dung đào tạo, bồi dưỡng kiến thức, kỹ năng về an ninh mạng, an toàn thông tin trong các chương trình giáo dục phổ thông phù hợp với từng cấp học; đồng thời định hướng, phối hợp với các cơ sở giáo dục đại học, cơ sở đào tạo trên địa bàn tích hợp, phát triển các chương trình đào tạo liên quan đến lĩnh vực an ninh mạng.

- Phối hợp với Công an tỉnh, các sở, ngành và cơ sở đào tạo tổ chức đào tạo, bồi dưỡng, phát triển nguồn nhân lực an ninh mạng chất lượng cao phục vụ nhu cầu của địa phương; tăng cường các hoạt động tuyên truyền, nâng cao nhận thức, kỹ năng sử dụng không gian mạng an toàn cho học sinh, sinh viên.

- Khuyến khích các cơ sở giáo dục triển khai các hoạt động ngoại khóa, cuộc thi, câu lạc bộ về an toàn thông tin, an ninh mạng; từng bước hình thành nguồn nhân lực có kiến thức, kỹ năng cơ bản, đáp ứng yêu cầu trong tình hình mới.

### **4. Sở Tài chính**

Căn cứ khả năng cân đối của ngân sách nhà nước và phân cấp ngân sách hiện hành; trên cơ sở đề nghị của các sở, ngành, địa phương có liên quan tham mưu cấp thẩm quyền trong việc bố trí nguồn kinh phí để thực hiện nội dung trong Kế hoạch theo quy định Luật Ngân sách nhà nước, Luật Đầu tư công và các văn bản hướng dẫn có liên quan.

### **5. Sở Nội vụ**

- Chủ trì, phối hợp với các cơ quan, đơn vị liên quan nghiên cứu, tham mưu Ủy ban nhân dân tỉnh xây dựng, hoàn thiện cơ chế, chính sách phát triển nguồn nhân lực trong lĩnh vực an ninh mạng, bảo đảm phù hợp với yêu cầu nhiệm vụ và định hướng phát triển của địa phương.

- Tham mưu UBND tỉnh bố trí, sắp xếp, kiện toàn tổ chức bộ máy và biên chế; xác định vị trí việc làm, tiêu chuẩn chức danh, cơ cấu ngạch công chức, viên chức gắn với nhiệm vụ bảo vệ an ninh mạng tại các cơ quan, đơn vị.

- Phối hợp rà soát, đề xuất kế hoạch tuyển dụng, sử dụng, đào tạo, bồi dưỡng và phát triển đội ngũ cán bộ, công chức, viên chức làm công tác an ninh mạng; bảo đảm đủ số lượng, nâng cao chất lượng, đáp ứng yêu cầu nhiệm vụ trong tình hình mới.

### **6. Các sở, ban, ngành, Ủy ban nhân dân các xã, phường**

- Căn cứ chức năng, nhiệm vụ được giao và nội dung của Kế hoạch, tổ chức triển khai cụ thể tại địa phương. Thực hiện chế độ thông tin, báo cáo định kỳ hoặc đột xuất về tình hình, kết quả triển khai gửi Công an tỉnh để tổng hợp, tham mưu theo quy định.

- Tổ chức triển khai các biện pháp bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý; từng bước xây dựng, kiện toàn lực lượng tham gia bảo vệ an ninh mạng tại cơ sở, bảo đảm phù hợp với điều kiện thực tế và yêu cầu nhiệm vụ.

- Chủ động phối hợp với các cơ quan chức năng trong công tác phòng ngừa, phát hiện, xử lý và khắc phục sự cố an ninh mạng xảy ra tại địa phương; tham gia đầy đủ các hoạt động của đội ứng cứu sự cố an ninh mạng của tỉnh, bảo đảm kịp thời, hiệu quả, hạn chế thấp nhất thiệt hại có thể xảy ra.

- Tổ chức triển khai, duy trì thực hiện các phương án bảo đảm an toàn thông tin theo cấp độ đã được phê duyệt, bảo đảm 100% hệ thống thông tin thuộc phạm vi quản lý tuân thủ quy định về bảo đảm an toàn thông tin; kịp thời khắc phục các tồn tại, hạn chế, nâng cao năng lực phòng ngừa, phát hiện và xử lý sự cố an ninh mạng.

## **7. Doanh nghiệp, tổ chức có liên quan**

- Chủ động phối hợp với các cơ quan nhà nước trên địa bàn tỉnh trong việc triển khai các giải pháp bảo đảm an ninh mạng, an toàn thông tin; tham gia chia sẻ thông tin, cảnh báo nguy cơ, hỗ trợ xử lý sự cố an ninh mạng theo quy định, góp phần bảo đảm an toàn, ổn định hoạt động trên không gian mạng.

- Ưu tiên nghiên cứu, đầu tư, phát triển và sử dụng các sản phẩm, giải pháp an ninh mạng “Make in Vietnam”; nâng cao năng lực tự chủ công nghệ, bảo đảm phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật và yêu cầu bảo đảm an ninh mạng.

- Phối hợp với các cơ quan chức năng, cơ sở đào tạo tham gia đào tạo, bồi dưỡng, phát triển nguồn nhân lực an ninh mạng; tích cực tham gia xây dựng và phát triển hệ sinh thái an ninh mạng tại địa phương, góp phần nâng cao năng lực chung về bảo vệ an ninh mạng.

- Thực hiện nghiêm các quy định của pháp luật về an ninh mạng, an toàn thông tin; triển khai các biện pháp kỹ thuật, nghiệp vụ nhằm bảo đảm an toàn hệ thống thông tin, hạ tầng viễn thông, dịch vụ số do doanh nghiệp quản lý, vận hành.

Giao Công an tỉnh chủ trì, phối hợp với các sở, ngành, địa phương theo dõi, đôn đốc việc triển khai thực hiện Kế hoạch, kịp thời báo cáo và kiến nghị UBND tỉnh các biện pháp cần thiết để bảo đảm thực hiện đồng bộ và có hiệu quả; đồng thời tổng hợp báo cáo theo quy định. Các cơ quan, đơn vị, địa phương triển khai thực hiện hiệu quả Kế hoạch này, quá trình triển khai, thực hiện, nếu có khó khăn, vướng mắc, các đơn vị, địa phương có văn bản gửi Công an tỉnh để tổng hợp và hướng dẫn giải quyết theo thẩm quyền hoặc trình cấp có thẩm quyền xem xét, quyết định./.

### **Nơi nhận:**

- Bộ Công an;
- Chủ tịch, các PCT UBND tỉnh;
- Các sở, ban, ngành tỉnh;
- UBND các xã, phường;
- Lãnh đạo VP UBND tỉnh;
- Các DN viễn thông: VNPT, Viettel, Mobifone, FPT;
- Lưu: VT, CVNC<sup>Tường</sup>.

**TM. ỦY BAN NHÂN DÂN**  
**KT. CHỦ TỊCH**  
**PHÓ CHỦ TỊCH THƯỜNG TRỰC**

**Nguyễn Lê Huy**

**Phụ lục**  
**DANH MỤC CÁC NHIỆM VỤ, GIẢI PHÁP TRIỂN KHAI ĐỀ ÁN “NÂNG CAO NĂNG LỰC  
 HOẠT ĐỘNG CỦA LỰC LƯỢNG BẢO VỆ AN NINH MẠNG QUỐC GIA”**

(Kèm theo Kế hoạch số /KH-UBND ngày tháng 4 năm 2026 của UBND tỉnh Hưng Yên)

STT	Nhiệm vụ	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian thực hiện	Ghi chú
1	Rà soát, cập nhật, hoàn thiện hành lang pháp lý, văn bản hướng dẫn công tác bảo đảm an ninh mạng theo thẩm quyền.	Công an tỉnh	Các sở, ngành, địa phương liên quan	Thường xuyên	
2	Tham mưu triển khai TCVN 11423:2025 trên cơ sở hợp nhất TCVN 11423:2025 và TCVN 11930:2017 cho các cấp độ hệ thống thông tin vận hành trên địa bàn tỉnh.	Công an tỉnh	Các sở, ngành, địa phương liên quan	Quý II/2026	Sau khi Bộ Công an ban hành tiêu chuẩn
3	Ban hành khung quản lý rủi ro an ninh mạng tỉnh, hướng dẫn các đơn vị trong quản lý rủi ro an ninh mạng.	Công an tỉnh	Các sở, ngành, địa phương liên quan	Quý IV/2026	Sau khi Bộ Công an ban hành Khung quản trị rủi ro an ninh mạng
4	Rà soát, đề xuất chính sách ưu đãi hỗ trợ doanh nghiệp đổi mới sáng tạo, làm chủ công nghệ, phát triển các sản phẩm, dịch vụ an ninh mạng trong nước.	Công an tỉnh	Sở Khoa học và Công nghệ, các sở, ngành, địa phương liên quan	Thường xuyên	
5	Kiện toàn Tiểu ban An ninh mạng tỉnh.	Công an tỉnh		Tháng 4/2026	
6	Rà soát, xây dựng tổ chức lực lượng bảo vệ an ninh mạng tại tỉnh.	Công an tỉnh			Sau khi có hướng dẫn của Bộ Công an
7	100% các hệ thống thông tin sử dụng vốn ngân sách nhà nước được triển khai đầy đủ các phương án bảo đảm an ninh mạng theo cấp độ.	Công an tỉnh	Các sở, ngành, địa phương liên quan	Quý II/2026	
8	Tổ chức đào tạo, bồi dưỡng, tập huấn, diễn tập nhằm nâng cao trình độ chuyên môn, kỹ năng nghiệp vụ và năng lực ứng phó, xử lý sự cố an ninh mạng, bảo đảm sẵn sàng đáp ứng yêu cầu trong mọi tình huống.	Công an tỉnh	Các sở, ngành, địa phương liên quan	Hằng năm	

9	Phổ biến, nâng cao kiến thức an ninh mạng cho người dân qua các nền tảng học tập số, “Bình dân học vụ số”, các khóa học đại chúng mở (MOOC) và các chiến dịch truyền thông đại chúng.	Công an tỉnh	Sở Khoa học và Công nghệ, Các sở, ngành, địa phương liên quan	Thường xuyên	
10	Triển khai áp dụng chỉ số đảm bảo an ninh mạng để đánh giá năng lực bảo đảm an ninh mạng của các cơ quan tổ chức, doanh nghiệp trên địa bàn.	Công an tỉnh	Các sở, ngành, địa phương liên quan	2026-2027	Sau khi Bộ Công an ban hành, hướng dẫn
11	Kết nối nền tảng theo dõi, điều hành an ninh mạng tỉnh vào nền tảng theo dõi, điều hành an ninh mạng quốc gia.	Công an tỉnh		2026-2027	
12	Trang bị hệ thống, công cụ chuyên dụng cho lực lượng bảo vệ an ninh mạng, tối thiểu gồm hệ thống, công cụ rà quét phát hiện lỗ hổng bảo mật; hệ thống, công cụ hỗ trợ điều tra số, ứng cứu, khắc phục sự cố an ninh mạng.	UBND tỉnh		Thường xuyên	
13	Thúc đẩy phát triển các trung tâm đo kiểm an ninh mạng theo hướng xã hội hóa, đủ năng lực thực hiện thử nghiệm, đánh giá sự phù hợp tiêu chuẩn, quy chuẩn đối với sản phẩm an ninh mạng.	Công an tỉnh	Các cơ quan, doanh nghiệp và hội, hiệp hội trong lĩnh vực an ninh mạng, CNTT.	2026-2027	Sau khi có hướng dẫn của Bộ Khoa học và Công nghệ, Bộ Công an