TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN 13266:2021

ISO/IEC 27042:2015

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN - CÁC KỸ THUẬT AN TOÀN - HƯỚNG DẪN PHÂN TÍCH VÀ GIẢI THÍCH BẰNG CHỨNG SỐ

Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence

HÀ NỘI – 2021

Mục lục

Lời nói đầu

TCVN 13266:2021 hoàn toàn tương đương ISO/IEC 27042:2015.

TCVN 13266:2021 do Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam (thuộc Cục An toàn thông tin) biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Tổng quát

Tiêu chuẩn này cung cấp hướng dẫn về việc tiến hành phân tích và giải thích các bằng chứng số tiềm năng để xác định và đánh giá bằng chứng số có thể được sử dụng để hỗ trợ thông tin về sự cố. Bản chất của dữ liệu và thông tin tạo nên bằng chứng số tiềm năng sẽ phụ thuộc vào bản chất của sự cố và các nguồn bằng chứng số liên quan đến sự cố đó.

Khi dùng tiêu chuẩn này người dùng ngầm định rằng đã tuân thủ các hướng dẫn đã đưa ra trong ISO/IEC 27035-2, TCVN ISO/IEC 27037:2019 và tất cả các quy trình sử dụng tương thích với hướng dẫn của TCVN ISO/IEC 27043:2019, TCVN ISO/IEC 27041:2019.

Mối quan hệ với các tiêu chuẩn khác

Tiêu chuẩn này nhằm bổ sung cho các tiêu chuẩn và tài liệu khác về hướng dẫn điều tra và chuẩn bị điều tra các sự cố an toàn thông tin. Đây không phải là một hướng dẫn toàn diện, nhưng đưa ra một số nguyên tắc cơ bản nhằm đảm bảo các công cụ, kỹ thuật và phương pháp có thể được lựa chọn thích hợp và được chỉ ra phù hợp với mục đích khi cần.

Tiêu chuẩn này cũng nhằm mục đích thông báo cho những người ra quyết định cần xác định độ tin cậy của bằng chứng số được trình bày với họ. Nó được áp dụng cho các tổ chức cần bảo vệ, phân tích và trình bày bằng chứng số tiềm năng. Nó thích hợp cho các cơ quan hoạch định chính sách tạo ra và đánh giá các thủ tục liên quan đến bằng chứng số, thường là một phần của một bằng chứng lớn hơn.

Tiêu chuẩn này mô tả một phần của quy trình điều tra toàn diện, bao gồm, nhưng không giới hạn với các chủ đề, lĩnh vực sau đây:

- Quản lý sự cố, bao gồm việc chuẩn bị và lập kế hoạch điều tra;
- Xử lý bằng chứng số;
- Việc sử dụng, và các vấn đề gây ra bởi, biên tập số;
- Hệ thống phát hiện và ngăn chặn chặn xâm nhập, bao gồm cả thông tin có thể thu được từ các hệ thống này;
- An toàn lưu trữ, bao gồm cả việc làm sạch dữ liệu hệ thống lưu trữ;
- Đảm bảo các phương pháp điều tra phù hợp với mục đích;
- Tiến hành phân tích và giải thích bằng chứng số;
- Hiểu được các nguyên tắc và quy trình về điều tra bằng chứng số;
- Quản lý sự kiện sự cố an toàn thông tin, bao gồm việc thu thập bằng chứng từ các hệ thống liên quan đến việc quản lý sự cố sự kiện an toàn thông tin;
- Mối quan hệ giữa phương pháp phát hiện điện tử và các phương pháp điều tra khác, cũng như việc sử dụng kỹ thuật phát hiện điện tử trong các cuộc điều tra khác;

- Quản trị điều tra, bao gồm điều tra pháp lý.

Các lĩnh vực này được đề cập từng phần trong các tiêu chuẩn sau:

- TCVN ISO/IEC 27037:2019

Tiêu chuẩn này mô tả các phương tiện mà những phương tiện này tham gia vào các giai đoạn đầu của cuộc điều tra, bao gồm ứng phó ban đầu, có thể đảm bảo bằng chứng số tiềm năng được thu thập đầy đủ để cho phép điều tra được tiến một cách thích hợp.

- ISO/IEC 27038

Một số tài liệu có thể chứa thông tin không được tiết lộ cho một số cộng đồng. Các tài liệu đã được sửa đổi có thể được phát hành cho các cộng đồng này sau khi xử lý thích hợp tài liệu gốc. Quá trình loại bỏ thông tin không được tiết lộ được gọi là "biên tập".

Việc biên tập các tài liệu kỹ thuật số là một lĩnh vực tương đối mới đối với thực tiễn quản lý tài liệu, gây ra các vấn đề nhất định và những rủi ro tiềm ẩn. Khi các tài liệu số được biên tập, các thông tin được loại bỏ phải đảm bảo không thể phục hồi được. Do đó cần phải chú ý đảm bảo rằng thông tin đã được biên tập phải được xóa vĩnh viễn khỏi tài liệu số (ví dụ: không được ẩn một cách đơn giản trong các phần không thể hiển thị của tài liệu).

ISO/IEC 27038 xác định các phương pháp cho biên tập đối với các tài liệu số. Tiêu chuẩn này cũng xác định các yêu cầu đối với phần mềm được sử dụng để biên tập.

- ISO/IEC 27040:2015

Tiêu chuẩn này cung cấp hướng dẫn kỹ thuật chi tiết về cách thức các tổ chức có thể xác định mức độ giảm thiểu rủi ro phù hợp bằng cách sử dụng phương pháp tiếp cận đã được chứng minh và nhất quán cho việc lập kế hoạch, thiết kế, lập tài liệu và thực hiện đảm bảo an toàn lưu trữ dữ liệu. An toàn hệ thống lưu trữ áp dụng để việc bảo vệ (an toàn) thông tin được lưu trữ và để bảo vệ thông tin được chuyển qua các liên kết truyền thông liên quan đến lưu trữ. An toàn lưu trữ bao gồm an toàn thiết bị và phương tiện, an toàn các hoạt động quản lý liên quan đến thiết bị và phương tiện, an toàn của ứng dụng và dịch vụ, và an toàn liên quan đến các người dùng cuối trong suốt thời gian tồn tại của các thiết bị và phương tiện, và sau khi kết thúc sử dụng.

Các cơ chế an toàn như mã hóa và xóa sạch dữ liệu có thể ảnh hưởng đến khả năng điều tra của điều tra viên bằng các cơ chế xáo trộn. Chúng phải được xem xét trước và trong qua trình thực hiện cuộc điều tra. Chúng cũng có thể đóng vai trò quan trọng để đảm bảo rằng việc lưu trữ tài liệu bằng chứng trong và sau cuộc điều tra đã được chuẩn bị đầy đủ và an toàn.

- TCVN ISO/IEC 27041:2019

Điều quan trọng là các phương pháp và các quy trình được triển khai trong suốt cuộc điều tra có thể được chỉ ra là một cách phù hợp. Tiêu chuẩn này cung cấp hướng dẫn về cách thức để cung cấp đảm bảo rằng các phương pháp và quy trình đáp ứng các yêu cầu của cuộc điều tra và đã được kiểm tra phù hợp.

- TCVN ISO/IEC 27043:2019

Tiêu chuẩn này xác định các nguyên tắc và quy trình cốt lõi chung căn bản việc điều tra sự cố và cung cấp mô hình khung cho tất cả các giai đoạn điều tra.

Các dự án tiêu chuẩn của ISO/IEC sau đây cũng đề cập đến từng phần, các chủ đề lĩnh vực được xác định ở trên và có thể dẫn đến việc xuất bản các tiêu chuẩn có liên quan tại một thời điểm sau khi xuất bản tiêu chuẩn này.

- ISO/IEC 27035 (tất cả các phần)

Tiêu chuẩn này gồm ba phần cung cấp cho các tổ chức một cách tiếp cận có cấu trúc và có kế hoạch để quản lý sự cố an toàn thông tin. Tiêu chuẩn này bao gồm:

- ISO/IEC 27035-1

Phần này trình bày các khái niệm này cơ bản và các bước quản lý sự cố an toàn thông tin. Nó kết hợp các khái niệm này với các nguyên tắc theo một cách tiếp cận có cấu trúc để phát hiện, báo cáo, đánh giá, ứng phó và áp dụng các bài học kinh nghiệm.

- ISO/IEC 27035-2

Phần này cung cấp các khái niệm để chuẩn bị và lập kế hoạch ứng phó sự cố. Các khái niệm bao gồm chính sách và kế hoạch quản lý sự cố, thành lập đội ứng phó sự cố, đào tạo và giao ban nâng cao nhận thức, được dựa trên kế hoạch và giai đoạn chuẩn bị theo mô hình được trình bày trong ISO/IEC 27035-1. Phần này cũng bao gồm pha "Bài học kinh nghiệm" của mô hình.

- ISO/IEC 27035-3

Phần này bao gồm trách nhiệm của nhân viên và các hoạt động thực hành ứng phó sự cố của toàn tổ chức. Tập trung đặc biệt dành cho các hoạt động của đội ứng cứu sự cố như bao gồm các hoạt động giám sát, phát hiện, phân tích và ứng phó để tập hợp dữ liệu hoặc sự kiện an toàn thông tin.

- ISO/IEC 27044

Tiêu chuẩn này hướng dẫn cho các tổ chức trong việc chuẩn bị triển khai quy trình/hệ thống quản lý thông tin và sự kiện an toàn thông tin. Cụ thể, tiêu chuẩn đề cập đến việc lựa chọn, triển khai và vận hành SIEM. Tiêu chuẩn này cung cấp hỗ trợ trong việc đáp ứng các yêu cầu của ISO/IEC 27001 liên quan đến việc thực hiện các quy trình và các biện pháp kiểm soát khác có khả năng cho phép phát hiện và ứng phó kịp thời với các sự cố an toàn thông tin, để thực hiện giám sát và rà soát các quy trình nhằm xác định đúng các lỗi vi phạm và sự cố an toàn.

- ISO/IEC 27050 (tất cả các phần)

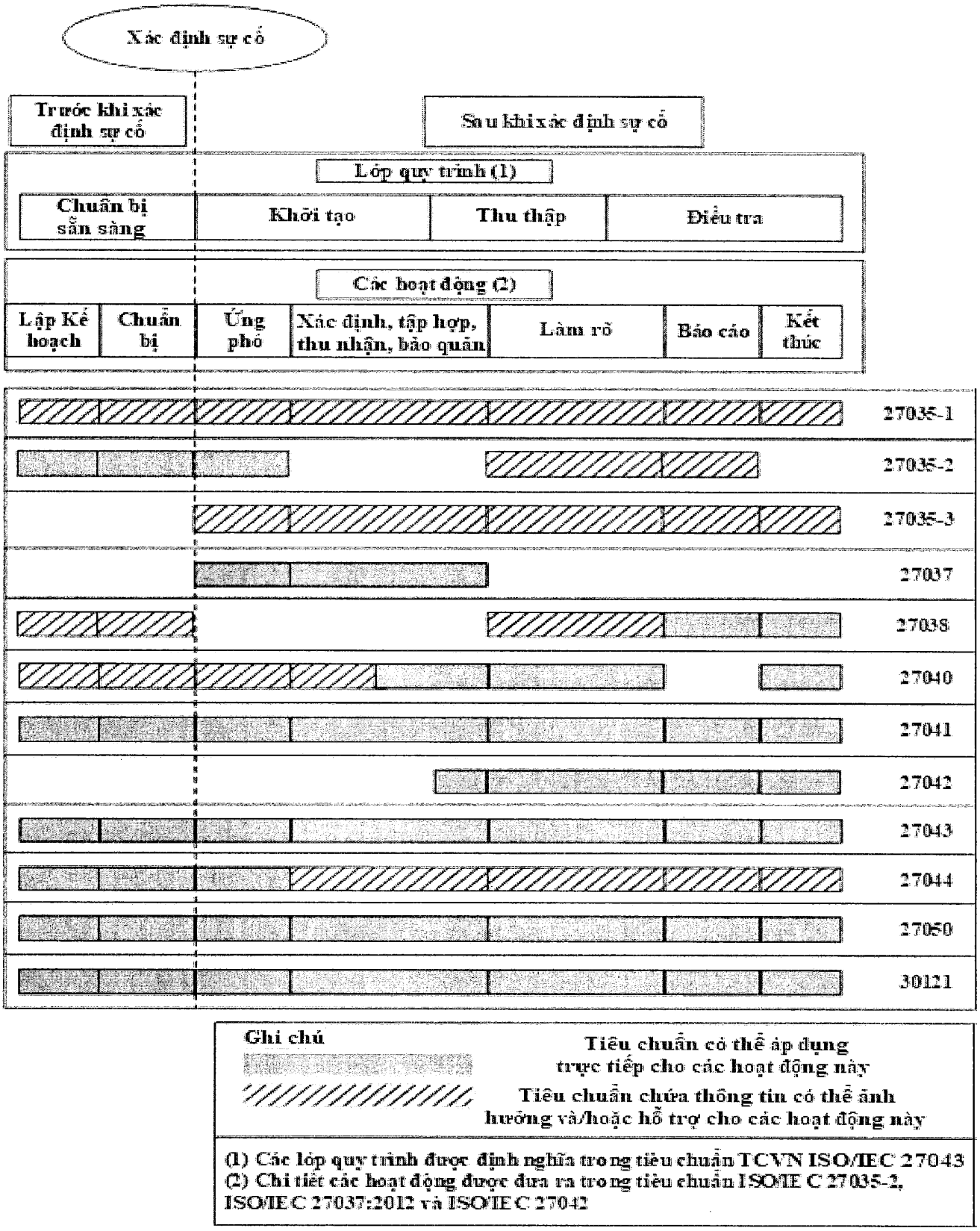
Tiêu chuẩn này đề cập đến các hoạt động trong khám phá điện tử, bao gồm, nhưng không giới hạn, việc xác định, bảo quản, tập hợp, xử lý, soát xét, phân tích, và tạo ra các thông tin lưu trữ điện tử (ESI). Bên cạnh đó, tiêu chuẩn này cung cấp hướng dẫn về các biện pháp, trải rộng từ sự khởi tạo ESI đến việc sắp đặt cuối cùng của chúng, mà tổ chức có thể thực hiện để giảm thiểu rủi ro và chi phí khám phá điện tử. Tiêu chuẩn này thích hợp cho cả nhân viên kỹ thuật và phi kỹ thuật có liên quan đến một số hoặc tất cả hoạt động khám phá điện tử. Điều quan trọng cần lưu ý là hướng dẫn này không được mâu thuẫn hoặc vi phạm các quy định pháp lý hoặc quy định nội bộ.

Khám phá điện tử thường phục vụ như là người chỉ lối cho các cuộc điều tra, cũng như các hoạt động thu thập bằng chứng và xử lý. Bên cạnh đó, tính nhạy cảm và quan trọng của dữ liệu đôi khi đòi hỏi bắt buộc bảo vệ như an toàn lưu trữ để chống lại sự vi phạm dữ liệu.

- ISO/IEC 30121:2015

Tiêu chuẩn này cung cấp khung mẫu cho các bộ phận quản trị của tổ chức (bao gồm cả chủ sở hữu, hội đồng thành viên, giám đốc, đối tác, giám đốc điều hành hoặc tương tự) cách tốt nhất để chuẩn bị một tổ chức cho việc điều tra số trước khi nó xảy ra. Tiêu chuẩn này áp dụng cho việc phát triển các quy trình chiến lược (các quyết định) liên quan đến việc duy trì, tính sẵn sàng, truy cập, sự hiệu quả về chi phí của việc tiết lộ bằng chứng số. Tiêu chuẩn này áp dụng cho tất cả các loại hình và các quy mô tổ chức. Sự sẵn sàng về pháp lý đảm bảo rằng một tổ chức đã thực hiện chiến lược chuẩn bị thỏa đáng và phù hợp cho việc chấp nhận các sự kiện tiềm năng của bản chất chứng cứ. Các hành động có thể xảy ra như kết quả của các hành vi xâm phạm an toàn, giả mạo và ảnh hưởng uy tín. Trong mọi tình huống, công nghệ thông tin (IT) phải được triển khai một cách chiến lược để tối đa hóa hiệu quả của tính sẵn sàng, khả năng tiếp cận và hiệu quả chi phí.

Hình 1 mô tả các hoạt động điển hình xung quanh một sự cố và việc điều tra sự cố. Những con số được hiển thị trong biểu đồ này (ví dụ: 27037) chỉ ra các tiêu chuẩn được liệt kê ở trên và các thanh bóng mờ hiển thị nơi có khả năng áp dụng trực tiếp hoặc có một số ảnh hưởng đối với quá trình điều tra (ví dụ: bằng cách thiết lập chính sách hoặc tạo ra các ràng buộc). Tuy nhiên tất cả các tiêu chuẩn này được khuyến khích xem xét trong các giai đoạn trước, và trong quá trình lập kế hoạch và chuẩn bị. Các lớp quy trình được trình bày đã được xác định đầy đủ trong tiêu chuẩn này và các hoạt động xác định phù hợp với chúng được nêu chi tiết trong tiêu chuẩn ISO/IEC 27035-2, TCVN ISO/IEC 27037:2019.



Hình 1 - Khả năng áp dụng các tiêu chuẩn đối với các lớp và hoạt động của quy trình điều tra sự cố

Công nghệ thông tin – Các kỹ thuật an toàn – Hướng dẫn phân tích và giải thích bằng chứng số

Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence

1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp hướng dẫn về phân tích và giải thích bằng chứng số theo cách giải quyết các vấn đề về tính liên tục, tính hiệu lực, tính tái tạo và tính lặp lại. Nó cung cấp tóm lược thực hành tốt nhất để lựa chọn, thiết kế, thực hiện các quy trình phân tích và ghi lại đầy đủ thông tin để cho phép các quy trình đó chịu sự giám sát độc lập khi được yêu cầu. Nó cung cấp hướng dẫn về các cơ chế phù hợp để chứng minh trình độ và năng lực của nhóm điều tra.

Phân tích và giải thích bằng chứng số có thể là một quá trình phức tạp. Trong một số trường hợp, có thể có một số phương pháp được áp dụng và các thành viên của nhóm điều tra sẽ được yêu cầu chứng minh sự lựa chọn của họ về một quy trình cụ thể và cho thấy nó tương đương với quy trình khác được sử dụng bởi các nhà điều tra khác. Trong các trường hợp khác, các nhà điều tra có thể phải nghĩ ra các phương pháp mới để kiểm tra bằng chứng số chưa được xem xét trước đây và phải có thể chỉ ra rằng phương pháp được tạo ra là phù hợp với mục đích.

Áp dụng một phương pháp cụ thể có thể ảnh hưởng đến việc giải thích bằng chứng số được xử lý bằng phương pháp đó. Bằng chứng số có sẵn có thể ảnh hưởng đến việc lựa chọn các phương pháp để phân tích sâu hơn về bằng chứng số đã được thu thập.

Tiêu chuẩn này cung cấp một khuôn mẫu chung, cho phân tích và giải thích các yếu tố của xử lý sự cố an toàn hệ thống thông tin, nó có thể được sử dụng để hỗ trợ thực hiện các phương pháp mới và cung cấp một tiêu chuẩn chung tối thiểu cho bằng chứng số được tạo ra từ các hoạt động đó.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 11238:2015 (ISO/IEC 2700:2014), Công nghệ thông tin - Kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng.

TCVN ISO/IEC 27037:2019, Công nghệ thông tin - Kỹ thuật an toàn - Hướng dẫn xác định, tập hợp, thu nhận và bảo quản bằng chứng số.

TCVN ISO/IEC 27041:2019, Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn đảm bảo sự phù hợp và đầy đủ của phương pháp điều tra sự cố.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN 11238:2015 (ISO/IEC 27000:2014) và các thuật ngữ, định nghĩa sau: