PHỤ LỤC 2. CÁC YÊU CẦU VỀ HẠ TẦNG KỸ THUẬT, TIÊU CHUẨN CÔNG NGHỆ THÔNG TIN ÁP DỤNG

1. Các tiêu chuẩn CNTT áp dụng cho Kiến trúc Chính quyền điện tử cấp Tỉnh

Các tiêu chuẩn CNTT đã được ban hành theo các văn bản quy phạm pháp luật, tỉnh Bình Phước và các cơ quan có liên quan lưu ý tuân thủ trong quá trình triển khai thực hiện Kiến trúc; với các tiêu chuẩn CNTT chưa được ban hành thì tỉnh sẽ đề xuất để Bộ Thông tin và Truyền thông ban hành, làm cơ sở triển khai Kiến trúc. Sau đây là các tiêu chuẩn CNTT áp dụng cho Kiến trúc Chính quyền điện tử tỉnh Bình Phước.

1.1. Tiêu chuẩn CNTT áp dụng cho Kiến Trúc Nghiệp Vụ

Khuyến nghị sử dụng các tiêu chuẩn sau trong quá trình phần tích, mô hình hoá quy trình nghiệp vụ

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
1	Mô hình hóa đối tượng	UML v2.5	Unified Modelling Language version 2.5	TT 39/2017/TT-BTTTT

1.2. Tiêu chuẩn CNTT áp dụng cho Kiến Trúc Ứng Dụng

Khuyến nghị áp dụng các tiêu chuẩn sau trong quá trình thiết kế và triển khai kiến trúc Ứng Dụng.

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
1	Truyền tệp tin	HTTP v1.1	Hypertext Transfer Protocol version 1.1	TT 39/2017/TT-BTTTT
		HTTP v1.1	Hypertext Transfer Protocol version 1.1	
		HTTP v2.0	Hypertext Transfer Protocol version 2.0	
		WebDAV	Web-based Distributed Authoring and Versioning	
2	An toàn truyền tệp tin	HTTPS	Hypertext Transfer Protocol Secure	TT 39/2017/TT-BTTTT
		FTPS	File Transfer Protocol Secure	
		SFTP	SSH File Transfer Protocol	
3	Chuẩn nội dung Web	HTML v4.01	Hypertext Markup Language version 4.01	TT 39/2017/TT-BTTTT

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
		WCAG 2.0	W3C Web Content Accessibility Guidelines (WCAG) 2.0	
		HTML 5	Hypertext Markup Language version 5	
4	Chuẩn nội dung Web mở rộng	XHTML v1.1	Extensible Hypertext Markup Language version 1.1	TT 39/2017/TT-BTTTT
5	Giao diện người dùng	CSS2	Cascading Style Sheets Language Level 2	TT 39/2017/TT-BTTTT
		CSS3	Cascading Style Sheets Language Level 3	
		XSL	Extensible Stylesheet Language version	
6	Dịch vụ Web	SOAP v1.2	Simple Object Access Protocol version 1.2	TT 39/2017/TT-BTTTT
7	Dịch vụ Web	WSDL V2.0	Web Services Description Language version 2.0	TT 39/2017/TT-BTTTT
8	Dịch vụ Web dạng RESTful	RESTful web service	Representational state transfer	TT 39/2017/TT-BTTTT
9	Chuẩn kết nối ứng dụng cổng thông tin điện tử	JSR 168	Java Specification Requests 168 (Portlet Specification)	TT 39/2017/TT-BTTTT
10	Chuẩn kết nối ứng dụng cổng thông tin điện tử	JSR 286	Java Specification Requests 286 (Portlet Specification)	TT 39/2017/TT-BTTTT
11	Chuẩn kết nối ứng dụng cổng thông tin điện tử	WSRP v1.0	Web Services for Remote Portlets version 1.0	TT 39/2017/TT-BTTTT
12	Chuẩn kết nối ứng dụng cổng thông tin điện tử	WSRP v2.0	Web Services for Remote Portlets version 2.0	TT 39/2017/TT-BTTTT

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
13	Chuẩn kho lưu trữ nội dung	JSR 170	Java Specification Requests 170 (Content Repository v1.0)	Chưa có
14	Chuẩn kho lưu trữ nội dung	JSR 283	Java Specification Requests 283 (Content Repository v2.0)	Chưa có
15	Trình diễn bộ kí tự	UTF-8	8-bit Universal Character Set (UCS)/Unicode Transformation Format	TT 39/2017/TT-BTTTT

1.3. Tiêu chuẩn CNTT áp dụng cho Kiến Trúc Dữ Liệu

Khuyến nghị áp dụng các tiêu chẩn sau trong quá trình thiết kế và triển khai kiến trúc Dữ Liệu.

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
1	Sơ đồ chủ đề XML	XTM	XML Topic Maps 1.0	Chưa có
2	Hệ thống phân cấp OWL	OWL	W3C Web Ontology Language	Chưa có
3	Sơ đồ phân loại dữ liệu	ISO 11179	ISO/IEC 11179 Metadata Registry (MDR) standard	Chưa có
4	Ngôn ngữ định dạng văn bản	XML v1.0 (5th Edition)	Extensible Markup Language version 1.0 (5th Edition)	TT 39/2017/TT-BTTTT
5	Ngôn ngữ định dạng văn bản	XML v1.1	Extensible Markup Language version 1.1	TT 39/2017/TT-BTTTT
6	Định nghĩa các lược đồ trong tài liệu XML	XML Schema V1.1	XML Schema version 1.1	TT 39/2017/TT-BTTTT
7	Trao đổi dữ liệu đặc tả tài liệu XML	XMI v2.4.2	XML Metadata Interchange version 2.4.2	TT 39/2017/TT-BTTTT
8	Văn bản	(.txt)	Định dạng Plain Text (.txt): Dành cho các tài liệu cơ bản không có cấu trúc	TT 39/2017/TT-BTTTT

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
9	Văn bản	(.rtf) v1.8, v1.9.1	Định dạng Rich Text (.rtf) phiên bản 1.8, 1.9.1: Dành cho các tài liệu có thể trao đổi giữa các nền khác nhau	TT 39/2017/TT-BTTTT
10	Văn bản	(.docx)	Định dạng văn bản Word mở rộng của Microsoft (.docx)	TT 39/2017/TT-BTTTT
11	Văn bản	(.pdf) v1.4, v1.5, v1.6, v1.7	Định dạng Portable Document (.pdf) phiên bản 1.4, 1.5, 1.6, 1.7: Dành cho các tài liệu chỉ đọc	TT 39/2017/TT-BTTTT
12	Văn bản	(.doc)	Định dạng văn bản Word của Microsoft (.doc)	TT 39/2017/TT-BTTTT
13	Văn bản	(.odt) v1.2	Định dạng Open Document Text (.odt) phiên bản 1.2	TT 39/2017/TT-BTTTT
14	Bảng tính	(.csv)	Định dạng Comma eparated Variable/Delimited (.csv): Dành cho các bảng tính cần trao đổi giữa các ứng dụng khác nhau.	TT 39/2017/TT-BTTTT
15	Bảng tính	(.xlsx)	Định dạng bảng tính Excel mở rộng của Microsoft (.xlsx)	TT 39/2017/TT-BTTTT
16	Bảng tính	(.xls)	Định dạng bảng tính Excel của Microsoft (.xls)	TT 39/2017/TT-BTTTT
17	Bảng tính	(.ods) v1.2	Định dạng Open Document Spreadsheets (.ods) phiên bản 1.2	TT 39/2017/TT-BTTTT
18	Trình diễn	(.htm)	Định dạng Hypertext Document (.htm): cho các trình bày được trao đổi thông qua các loại trình duyệt khác nhau	TT 39/2017/TT-BTTTT

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
19	Trình diễn	(.pptx)	Định dạng PowerPoint mở rộng của Microsoft (.pptx)	TT 39/2017/TT-BTTTT
20	Trình diễn	(.pdf)	Định dạng Portable Document (.pdf): cho các trình bày lưu dưới dạng chỉ đọc	TT 39/2017/TT-BTTTT
21	Trình diễn	(.ppt)	Định dạng PowerPoint (.ppt) của Microsoft	TT 39/2017/TT-BTTTT
22	Trình diễn	(.odp) v1.2	Định dạng Open Document Presentation (.odp) phiên bản 1.2	TT 39/2017/TT-BTTTT
23	Dịch vụ Web	SOAP v1.2	Simple Object Access Protocol version 1.2	TT 39/2017/TT-BTTTT
24	Dịch vụ Web	WSDL V2.0	Web Services Description Language version 2.0	TT 39/2017/TT-BTTTT
25	Dịch vụ Web	UDDI v3	Universal Description, Discovery and Integration version 3	TT 39/2017/TT-BTTTT
26	Dịch vụ Web dạng RESTful	RESTful web service	Representational state transfer	TT 39/2017/TT-BTTTT

1.4. Tiêu chuẩn CNTT áp dụng cho Kiến Trúc Tích Hợp, Liên Thông

Khuyến nghị áp dụng các tiêu chẩn sau trong quá trình thiết kế và triển khai kiến trúc Tích Hợp, Liên Thông.

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
1	Ngôn ngữ định dạng văn bản	XML v1.0 (5th Edition)	Extensible Markup Language version 1.0 (5th Edition)	TT 39/2017/TT-BTTTT
2	Ngôn ngữ định dạng văn bản	XML v1.1	Extensible Markup Language version 1.1	TT 39/2017/TT-BTTTT
3	Định nghĩa các lược đồ trong tài liệu XML	XML Schema V1.1	XML Schema version 1.1	TT 39/2017/TT-BTTTT
4	Trao đổi dữ liệu đặc tả tài liệu XML	XMI v2.4.2	XML Metadata Interchange version 2.4.2	TT 39/2017/TT-BTTTT
5	Truyền tệp tin	HTTP v1.1	Hypertext Transfer Protocol version 1.1	TT 39/2017/TT-BTTTT
		HTTP v1.1	Hypertext Transfer Protocol version 1.1	
		HTTP v2.0	Hypertext Transfer Protocol version 2.0	
		WebDAV	Web-based Distributed Authoring and Versioning	
6	An toàn truyền tệp tin	HTTPS	Hypertext Transfer Protocol Secure	TT 39/2017/TT-BTTTT
		FTPS	File Transfer Protocol Secure	
		SFTP	SSH File Transfer Protocol	
7	Dịch vụ Web	SOAP v1.2	Simple Object Access Protocol version 1.2	TT 39/2017/TT-BTTTT
8	Dịch vụ Web	WSDL V2.0	Web Services Description Language version 2.0	TT 39/2017/TT-BTTTT

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
9	An toàn cho dịch vụ Web	WS-Security v1.1.1	Web Services Security: SOAP Message Security Version 1.1.1	TT 39/2017/TT-BTTTT
10	Dịch vụ Web	UDDI v3	Universal Description, Discovery and Integration version 3	TT 39/2017/TT-BTTTT
11	Dịch vụ Web dạng RESTful	RESTful web service	Representational state transfer	TT 39/2017/TT-BTTTT
12	An toàn trao đổi bản tin XML	XML Encryption Syntax and Processing	XML Encryption Syntax and Processing	TT 39/2017/TT-BTTTT
13		XML Signature Syntax and Processing	XML Signature Syntax and Processing	TT 39/2017/TT-BTTTT
14	Giải pháp xác thực người sử dụng	SAML v2.0	Security Assertion Markup Language version 2.0	TT 39/2017/TT-BTTTT
15	Xác thực và phân quyền	OAuth 2.0	OAuth 2.0 Authorization Framework	Chưa có
16		OpenID		Chưa có
17		RADIUS		Chưa có
18		Kerberos		Chưa có
19		Access Control Service		Chưa có
20	Truy cập thư mục	LDAP v3	Lightweight Directory Access Protocol version 3	TT 39/2017/TT-BTTTT
		X500		Chưa có
21	Giao vận mạng có kết nối	TCP	Transmission Control Protocol	TT 39/2017/TT-BTTTT

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
22	Mô hình hoá quy trình nghiệp vụ	BPMN v2.0	BPMN Specification - Business Process Model and Notation	Chưa có
23	Ngôn ngữ thực hiện quy trình nghiệp vụ thông qua Web Service	WS-BPEL 2.0	Web Services Business Process Execution Language	Chưa có
24	Giao thức tích hợp	JMS	Java Message Service	Chưa có
25		RMI	Java Remote Method Invocation	Chưa có
26		MQ	Message Queue	Chưa có
27		CORBA	Common Object Request Broker Architecture	Chưa có
28		DCOM	Distributed Component Object Model	Chưa có

1.5. Tiêu chuẩn CNTT áp dụng cho Kiến Trúc Bảo Mật

Khuyến nghị áp dụng các tiêu chẩn sau trong quá trình thiết kế và triển khai kiến trúc Tích Hợp, Liên Thông.

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
1	An toàn tầng giao vận	SSH v2.0	Secure Shell version 2.0	TT 39/2017/TT-BTTTT
2	An toàn tầng giao vận	TLS v1.2	Transport Layer Security version 1.2	TT 39/2017/TT-BTTTT
3	An toàn trao đổi bản tin XML	XML Encryption Syntax and Processing	XML Encryption Syntax and Processing	TT 39/2017/TT-BTTTT
4		XML Signature Syntax and Processing	XML Signature Syntax and Processing	TT 39/2017/TT-BTTTT

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
5	An toàn cho dịch vụ Web	WS-Security v1.1.1	Web Services Security: SOAP Message Security Version 1.1.1	TT 39/2017/TT-BTTTT
6	Tường lửa các ứng dụng web	WAF	Web Application Firewalls	Chưa có
7	An toàn tầng giao vận	SSH v2.0	Secure Shell version 2.0	TT 39/2017/TT-BTTTT
8	An toàn truyền tệp tin	HTTPS	Hypertext Transfer Protocol Secure	TT 39/2017/TT-BTTTT
		FTPS	File Transfer Protocol Secure	
		SFTP	SSH File Transfer Protocol	TT 39/2017/TT-BTTTT
9	Giải thuật mã hóa	TCVN 7816:2007	Công nghệ thông tin. Kỹ thuật mật mã thuật toán mã dữ liệu AES	TT 39/2017/TT-BTTTT
10		3DES	Triple Data Encryption Standard	
11		PKCS #1 V2.2	RSA Cryptography Standard - version 2.2	TT 39/2017/TT-BTTTT
12		ECC	Elliptic Curve Cryptography	TT 39/2017/TT-BTTTT
13	Giải thuật chữ ký số	PKCS #1 V2.2	RSA Cryptography Standard - version 2.2	TT 39/2017/TT-BTTTT
		ECDSA	Elliptic Curve Digital Signature Algorithm	
14	Giải thuật băm cho chữ ký số	SHA-2	Secure Hash Algorithms-2	TT 39/2017/TT-BTTTT
15	Giải thuật truyền khóa	RSA-KEM	Rivest-Shamir-Adleman - KEM (Key Encapsulation Mechanism) Key Transport Algorithm	TT 39/2017/TT-BTTTT

STT	Loại tiêu chuẩn	Ký hiệu tiêu chuẩn	Tên đầy đủ của tiêu chuẩn	Văn bản quy định
		ECDHE	Elliptic Curve Diffie Hellman Ephemeral	
16	Cú pháp thông điệp mật mã cho ký và mã hóa	PKCS#7 v1.5 (RFC 2315)	Cryptographic message syntax for file-based signing and encrypting version 1.5	TT 39/2017/TT-BTTTT
17	Cú pháp thông tin thẻ mật mã	PKCS#15 v1.1	Cryptographic token information syntax version 1.1	TT 39/2017/TT-BTTTT
18	Giao diện thẻ mật mã	PKCS#11 v2.20	Cryptographic token interface standard version 2.20	TT 39/2017/TT-BTTTT
19	Khuôn dạng danh sách chứng thư số thu hồi	RFC 5280	Certificate Revocation List Profile	TT 39/2017/TT-BTTTT
20	Khuôn dạng chứng thư số	RFC 5280	Public Key Infrastructure Certificate	TT 39/2017/TT-BTTTT
21	Cú pháp yêu cầu chứng thực	PKCS#10 v1.7 (RFC 2986)	Certification Request Syntax Specification version 1.7	TT 39/2017/TT-BTTTT
22	Giải pháp xác thực người sử dụng	SAML v2.0	Security Assertion Markup Language version 2.0	TT 39/2017/TT-BTTTT
23	Tiêu chuẩn ISO về việc quản lý bảo mật thông tin	ISO 27001	ISO/IEC 27001 - Information security management	Chưa có
24		ISO 27002	ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls	Chưa có

1.6. Tiêu chuẩn CNTT áp dụng cho Datacenter

- Thông tư số 03/2013/TT-BTTTT ngày 22/01/2013 của Bộ trưởng Bộ Thông tin và Truyền thông quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm dữ liệu.

- ISO 11801 Ed.2: CNTT - Hệ thống cáp chung dành cho khách hàng.

- AAS/ACIF S009: Quy định về lắp đặt cáp (Quy định thi công).

- AS/NZS 3080: Tích hợp hệ thống Cáp thông tin cho tòa nhà thương mại.

- AS/NZA 3084: Tiêu chuẩn về hệ thống máng, ống bảo vệ và không gian cho hệ thống Cáp thông tin trong tòa nhà thương mại.

- AS/NZS 3085.1: Các quy định cơ bản về quản lý hệ thống Cáp thông tin.

- AS/NZS 3087: Đo kiểm hệ thống cáp cân bằng.

- AS/NZS 4117: Thiết bị bảo vệ điện áp dành cho các ứng dụng viễn thông.

2. Kiến Trúc Hạ Tầng của Kiến trúc Chính quyền điện tử cấp tỉnh

2.1. Nguyên tắc xây dựng kiến trúc hạ tầng của tỉnh

- Triển khai đảm bảo theo tiêu chuẩn, quy chuẩn, quy định của Nhà nước và thế giới.

- Các thành phần đảm bảo khả năng triển khai, nâng cấp dễ dàng, không phụ thuộc vào bất kỳ một nền tảng kỹ thuật công nghệ nào.

- Hệ thống đảm bảo khả năng triển khai linh hoạt, dễ dàng.

- Các thành phần kỹ thuật cần đảm bảo các cơ chế bảo mật an toàn, an ninh thông tin theo các mức độ, thành phần khác nhau.

- Đảm bảo áp dụng các công nghệ mới, tiên tiến.

- Đảm bảo khả năng sẵn sàng, độ tin cậy cao.

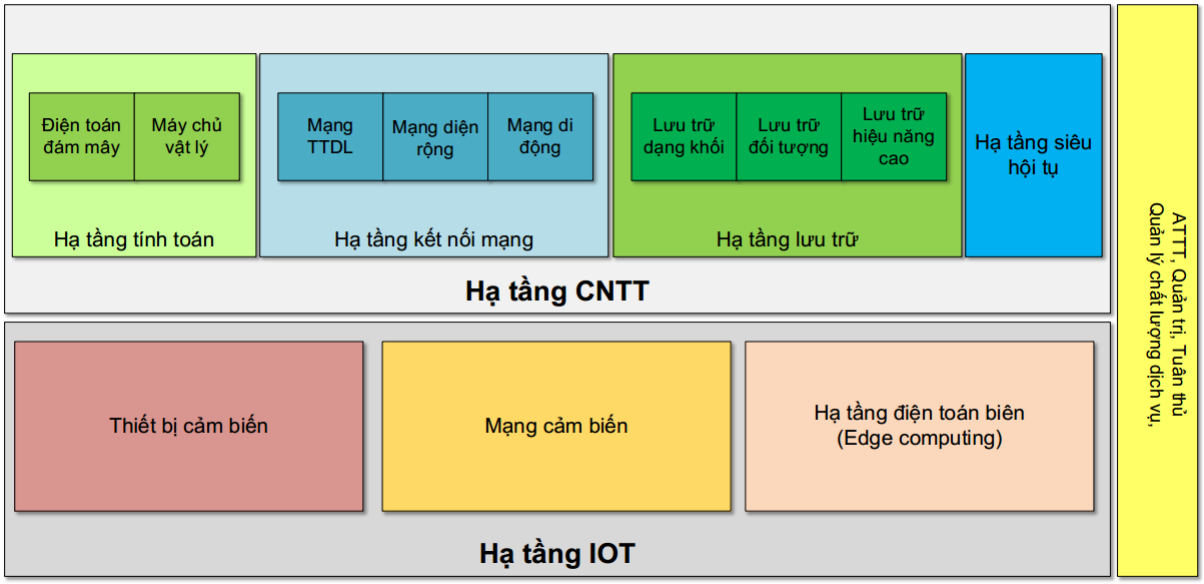
- Đảm bảo khả năng sử dụng, quản lý linh hoạt, dễ dàng.

- Việc đầu tư, nâng cấp hạ tầng kỹ thuật phải đảm bảo tiết kiệm, tránh đầu tư trùng lặp, lãng phí.

Ngoài ra, Các chương trình, nhiệm vụ, dự án liên quan đến triển khai, xây dựng, nâng cấp, mở rộng liên quan đến hạ tầng công nghệ thông tin phải có ý kiến của Sở Thông tin và Truyền thông tỉnh Bình Phước để đảm bảo phù hợp với Kiến trúc Chính phủ điện tử tỉnh Bình Phước.

2.2. Mô hình kiến trúc hạ tầng tổng thể tỉnh Bình Phước

Với độ phức tạp về yêu cầu đối với hạ tầng CNTT đến từ Kiến trúc ứng dụng, Kiến trúc dữ liệu, khả năng mở rộng, tính sẵn sàng cao, các yêu cầu về quản lý chất lượng dịch vụ, khả năng tuân thủ cũng như việc vận hành hạ tầng công nghệ thông tin cho thấy không có duy nhất một kiến trúc duy nhất nào đáp ứng được, chưa kể đến các yêu cầu đến từ các lĩnh vực ứng dụng và thiết bị IoT thiết thực phục vụ vận hành và quản lý đô thị thông minh trong tương lai. Vì thế, khi xây dựng Kiến trúc hạ tầng CNTT của tỉnh sẽ tiếp cận theo cách xây dựng từng khối hạ tầng hoặc kiến trúc hạ tầng và cung cấp dưới dạng dịch vụ, đi kèm với các tiêu chuẩn về kiểm soát, chất lượng dịch vụ, an toàn an ninh thông tin nhằm đảm bảo đáp ứng các yêu cầu hiện tại và tương lai.



Kiến trúc hạ tầng CNTT được chia làm 04 khối:

(1) Hạ tầng tính toán:

- Cung cấp năng lực xử lý thông tin, dữ liệu, vận hành ứng dụng... đa dạng về nhu cầu.

- Hầu như tất cả hoạt động về CNTT đều có nhu cầu về tính toán, đặc biệt là vận hành các ứng dụng, xử lý và phân tích thông tin.

- Với các xu hướng phát triển về nhu tính toán gần đây như trí tuệ nhân tạo, máy học, v.v., yêu cầu về tải đối với năng lực tính toán tăng càng lúc càng nhanh, gần như tuyến tính và trong một số trường hợp khả năng tính toán về CPU không còn đủ khả năng đáp ứng mà cần phải kết hợp với tính toán bằng chip xử lý đồ họa (GPU).

* Điện toán đám mây - Cloud computing:

- Phục vụ các nhu cầu tính toán thông thường, không cần hiệu năng quá cao và được cung cấp dưới dạng dịch vụ. Vì đặc thù của việc chia sẻ tài nguyên và mật độ ứng dụng trên mỗi đơn vị máy chủ vật lý nên nền tảng điện toán đám mây sẽ không phù hợp với các nhu cầu đặc thù như quản trị CSDL, máy học, lưu trữ... Tuy nhiên sẽ đủ sức đáp ứng các nhu cầu thông thường khác.

- Việc tích hợp sẵn các phần mềm quản trị, công cụ theo dõi giúp hạ tầng điện toán đám mây có khả năng giúp người dùng cuối tự phục vụ (self-service), giảm bớt các yêu cầu vận hành đơn giản và khả năng mở rộng khi cần gần như không giới hạn.

- Đáp ứng các nhu cầu về các platform thông dụng, các nền tảng xây dựng và vận hành ứng dụng đến từ kiến trúc ứng dụng và kiến trúc dữ liệu thông thường. Hầu hết các ứng dụng và dữ liệu sẽ vận hành trên hạ tầng này trong tương lai.

* Máy chủ vật lý:

- Đối với một số trường hợp rất đặc thù như nhu cầu xử lý hình ảnh dữ liệu công dân, tội phạm, giao thông, hoặc phân tích lượng lớn thông tin đến từ hạ tầng đô thị thông minh sẽ cần đến năng lực xử lý rất lớn hoặc rất đặc biệt như: GPU base computing; Deep-learning; In-memory computing. Do đặc thù về yêu cầu bảo mật, xử lý, cũng như đặc thù về công nghệ của các ứng dụng

trong các mảng này, tỉnh có thể cần có hạ tầng máy chủ vật lý đặc thù. Tuy nhiên việc thiết kế hạ tầng máy chủ vật lý phục vụ các yêu cầu tải trên nền tảng máy chủ vật lý (bare-metal) vẫn phải có khả năng quản lý như hạ tầng điện toán đám mây theo dạng "Infrastructure-as-a-service".

(2) Hạ tầng kết nối mạng

- Cung cấp khả năng kết nối các thiết bị, bao gồm cả kết nối giữa hạ tầng tính toán với hạ tầng lưu trữ, hạ tầng tính toán với người dùng, với các hạ tầng internet vạn vật (IoT).

- Số lượng thiết bị cần được kết nối, cùng với nhu cầu về an ninh, bảo mật, là một thách thức cực lớn đối với hạ tầng kết nối mạng.

- Không một mạng truyền thông đơn lẻ nào có thể cung cấp kết nối cho tất các hệ thống CNTT và IoT, mà phải tối thiểu bao gồm 03 hạ tầng mạng sau:

* Hạ tầng mạng trung tâm dữ liệu: Có tính sẵn sàng cao, độ trễ rất thấp, cung cấp hạ tầng kết nối cho:

+ Hạ tầng tính toán với hạ tầng lưu trữ;

+ Hạ tầng tính toán với người dùng cuối;

+ Hạ tầng tính toán với hạ tầng tính toán biên (edge computing).

- Một trong những thách thức lớn nhất của hạ tầng mạng trung tâm dữ liệu chính là hạ tầng điện toán đám mây.

- Không có một mạng truyền thông đơn lẻ nào có thể cung cấp kết nối cho tất cả các hệ thống t ĐTTM nên hoạch định về mạng truyền thông cho ĐTTM cần cân nhắc đến các vấn đề sau:

+ Giảm thiểu số lượng hệ thống mạng: Cần tìm kiếm các giải pháp mạng đa năng hơn là tạo ra một tập hợp nhiều hệ mạng riêng;

+ Phân tích và đánh giá hiệu suất, khả năng hoạt động của các mạng công cộng hay mạng dùng chung trước khi đầu tư xây dựng hệ thống mạng kết nối riêng. Ví dụ, mạng di động hoàn toàn có khả năng cung cấp kết nối cho các hệ thống kiểm soát điện lưới thông minh, giao thông thông minh, hệ thống cấp nước thông minh;

+ Khuyến khích nhận biết, hoạch định, thiết kế các bài toán liên ngành (cross-department) để có thể xác định các mảng, ngành nào có thể chia sẻ chung một network;

+ Xem xét tính khả thi của công nghệ khi tích hợp (băng thông, độ trễ, tính sẵn sàng, tính khả mở...);

+ Người dân có thể dễ dàng kết nối với các dịch vụ công qua nhiều phương thức kết nối khác nhau: Mạng cáp internet, mạng di động, IPTV, tin nhắn...;

+ Khuyến khích doanh nghiệp đầu tư vào xây dựng và cung cấp dịch vụ vận hành, hỗ trợ kỹ thuật, bảo trì cho hệ thống mạng của Tỉnh;

+ Cân nhắc chọn lựa các công cụ quản lý: Ưu tiên các công cụ quản lý tập trung, có khả năng quản lý đa dạng các công nghệ truyền thông khác nhau.

- Mạng được định nghĩa bằng phần mềm (Software-Define Network) được đề xuất là kiến trúc mạng của CQĐT và xa hơn là ĐTTM.

* Hạ tầng mạng diện rộng (WAN):

- Kết nối giữa các cơ quan chính quyền, người dân, các đơn vị cung cấp dịch vụ, các trung tâm dữ liệu với nhau... Đây là hạ tầng mạng cần khuyến khích các doanh nghiệp và tư nhân đầu tư, không chỉ phục vụ CQĐT mà còn phục vụ cho các hoạt động kinh doanh phát triển kinh tế.

- Cung cấp mạng trục, kết nối và liên thông các Sở/ban/ngành.

- Khả năng kết nối với các hệ thống mạng IoT để thu thập thông tin, giám sát, điều phối, tự động hóa...

- Khai thác kết nối giữa các mạng công cộng như mạng cáp internet, mạng di động, mạng truyền hình để tương tác với chính quyền, hỗ trợ trực tuyến, thông báo sự cố, bầu cử trực tuyến, thực hiện các thủ tục hành chính, v.v,...

- Tính tương tác giữa nhiều hạ tầng mạng chính là thử thách lớn nhất của hạ tầng mạng diện rộng.

- Để bảo đảm sự kết nối, tương tác giữa các thiết bị/công nghệ/giải pháp/hệ thống khác nhau của các hãng sản xuất khác nhau, bảo vệ chi phí đầu tư, hạn chế rủi ro, các thiết bị, công nghệ được lựa chọn cần phải tuân thủ các tiêu chuẩn mở (open standards) của thế giới.

- Tùy theo mảng thiết bị/công nghệ/giải pháp mà có các chuẩn mở khác nhau cần phải tuân thủ. Ví dụ như nếu đề cập đến công nghệ networking thì cần phải lưu ý đến các chuẩn của IEEE (LAN, WAN, Wireless, Bluetooth, RFID). Ngoài ra còn có các chuẩn của IEC, IETF, ANSI, ITU...Trên thực tế một loại thiết bị/công nghệ có thể có nhiều tiêu chuẩn mở khác nhau tùy vào yêu cầu, cách thức sử dụng, môi trường/ điều kiện/ khu vực địa lý sử dụng.

* Hạ tầng mạng tại các đơn vị:

- Là mạng nội bộ (LAN), cung cấp kết nối cho người dùng và thiết bị đầu cuối tại các đơn vị Sở/ Ban / Ngành. Người dùng có thể truy cập vào mạng nội bộ bằng mạng không dây hoặc mạng có dây. Mạng nội bộ của các đơn vị phải có khả năng kết nối đến TTDL của tỉnh với tính sẵn sàng cao: kết nối qua mạng Metronet của Tỉnh và kết nối từ internet thông qua kỹ thuật tạo mạng riêng ảo. Thông tin truyền dẫn giữa các đơn vị với TTDL phải được mã hóa.

- Thiết kế mạng nội bộ cần hướng đến khả năng hợp nhất truy cập và quản trị (truy cập và quản trị mạng có dây hay không dây như một hạ tầng thống nhất).

- Thiết kế mạng nội bộ phải đảm bảo hiệu năng phù hợp, có tính sẵn sàng cao, có khả năng chịu lỗi kể cả khi xảy ra các sự cố hỏng hóc về phần cứng.

- Thiết kế mạng nội bộ phải đảm bảo khả năng bảo mật nhiều lớp: Bảo mật đầu cuối (giải pháp chống thất thoát, tường lửa cá nhân, tính năng phát hiện và chống xâm nhập đầu cuối, phòng chống virus...), phân tách và kiểm soát giữa các lớp mạng nội bộ cũng như bên ngoài mạng (VLAN, tường lửa, proxy...) , khả năng phát hiện chống tấn công và xâm nhập (IPS), khả năng hiện thị, kiểm soát và ghi nhật kí (ví dụ như netflow, syslog, hardware DPI...).

- Mạng nội bộ có khả năng đáp ứng tốt các dịch vụ như hội họp trực tuyến, dịch vụ thoại bằng IP, dịch vụ truyền hình IP hay các ứng dụng truyền thông theo thời gian thực khác.

- Có khả năng ảo hóa mạng chuyển mạch cũng như hỗ trợ tốt cho các nền tảng ảo hóa khác.

Một số tiêu chuẩn quốc tế/giao thức tối thiểu mà mạng nội bộ cần phải hỗ trợ:

+ Giao thức mạng: IPv4, IPv6.

+ Về khả năng hỗ trợ cấu hình đơn giản: 802.1AF, CDP, LLDP, LLDP-MED.

+ Về bảo mật: IBNS (802.1X), (CISF): port security, DHCP snooping, DAI, IPSG.

+ Định danh: 802.1X, MAB, Web-Auth.

+ Dịch vụ kiểm soát mạng thông minh: PVST+, Rapid PVST+, EIGRP, OSPF, DTP, PAgP/LACP, UDLD, FlexLink, Portfast, UplinkFast, BackboneFast, LoopGuard, BPDUGuard, Port Security, RootGuard

+ Các giao thức đảm bảo tính sẵn sàng cao: HSRP, GLBP, VRRP.

+ Nguồn điện: PoE

* Hạ tầng mạng di động:

- Với sự bùng nổ của các thiết bị di động và hầu hết người dân đều trang bị điện thoại thông minh và có khả năng kết nối interrnet, hạ tầng mạng di động đóng vai trò không nhỏ trong việc cung cấp kết nối người dân với CQĐT với các ứng dụng công. Không chỉ dừng lại ở cung cấp internet cho các thiết bị di động, hạ tầng mạng di động còn đóng góp một phần không nhỏ trong việc cung cấp kết nối cho hạ tầng IoT, đặc biệt là các cảm biến.

- Kết hợp giữa bản đồ thông tin của TP và việc hệ thống hóa toàn bộ các hệ thống mạng, công nghệ mạng đang sử dụng để xem xét khả năng tận dụng hạ tầng mạng giữa các ngành với nhau (ví dụ: Nhiều ngành có thể dùng chung mạng camera, sensors, mạng phục vụ công tác quản lý, điều hành; tận dụng mạng di động sẵn có để truyền tải tín hiệu phù hợp...).

(3) Hạ tầng lưu trữ

* Hạ tầng lưu trữ dạng block:

- Phục vụ hạ tầng điện toán đám mây và hạ tầng máy chủ vật lý. Cung cấp tài nguyên cho các ứng dụng truyền thống thông thường, ví dụ như: máy chủ ảo, lưu trữ cơ sở dữ liệu nhỏ. Đây là hạ tầng lưu trữ cơ bản, phục vụ chủ đạo cho hầu hết các nền tảng và ứng dụng CNTT trong CQĐT và ĐTTM.

- Xu hướng công nghệ all-flash, lưu trữ bằng chip nhớ gần đây giúp cho hầu hết các thiết bị xây dựng hạ tầng lưu trữ dạng block có khả năng thích nghi với mật độ sử dụng của hạ tầng tính toán, đặc biệt là hạ tầng điện toán đám mây.

* Hạ tầng lưu trữ đối tượng (object):

- Phát sinh từ nhu cầu thực tế về đô thị thông minh, IoT, hoặc các nhu cầu về lưu trữ hay xử lý video CCTV, an ninh, phân tích hình ảnh, video.

- Cung cấp dung lượng lưu trữ rất lớn (petabyte, exabyte scales).

- Một trong nhưng lý do để tách biệt giữa hạ tầng lưu trữ dạng block và hạ tầng lưu trữ đối tượng nhằm giảm chi phí và giảm overhead trong việc lưu trữ các dữ liệu khá đặc thù, không cần hiệu suất cao như đã đề cập ở trên.

Do nhu cầu khá đặc thù, hiện tại có thể chưa cần đầu tư, tuy nhiên về lâu dài đây sẽ là xu hướng tất yếu, đặc biệt vì nhu cầu lưu trữ dữ liệu càng lúc càng tăng và sẽ càng tăng nhanh khi hạ tầng mạng IoT phục vụ đô thị thông minh bắt đầu được triển khai.

* Hạ tầng lưu trữ hiệu năng cao: Phục vụ các yêu cầu rất đặc biệt như xử lý thông tin trong bộ nhớ (in-memory) hoặc các workload như CSDL, Data warehouse. Bao gồm các thiết bị lưu trữ với dung lượng thấp đến trung bình như có băng thông rất cao và độ trễ rất thấp. Với công nghệ rất đặc thù và dung lượng lưu trữ thấp nên hạ tầng lưu trữ hiệu năng cao chỉ nên được đầu tư tương ứng với nhu cầu phát sinh từ các ứng dụng đặc biệt như:

+ Phân tích dữ liệu từ IoT đối với các ngành Giao thông, Y tế, Môi trường...;

+ Phân tích các báo cáo tài chinh;

+ Trí thông minh nhân tạo, máy học, hệ thống ra quyết định trong lĩnh vực an ninh, nhân diện khuôn mặt, giọng nói, v.v.

(4) Hạ tầng hội tụ/siêu hội tụ/tích hợp: Với sự đa dạng từ nhu cầu đơn giản đến phức tạp cũng như các yêu cầu thực tế trong vận hành hạ tầng CNTT thì Kiến trúc về hạ tầng CNTT truyền thống không thể đáp ứng, chỉ có Kiến trúc hạ tầng hội tụ/siêu hội tụ/tích hợp có khả năng này.

* Quản lý hạ tầng trung tâm điện toán đám mây:

- Dựa trên nền tảng phần mềm (software-defined) để vận hành, tự động hóa, giảm thiểu độ phức tạp trong quá trình vận hành nhưng vẫn đảm bảo được khả năng tách biệt, các yêu cầu về cung cấp dịch vụ và quản lý chất lượng dịch vụ.

-Trong thực tế vận hạnh Trung tâm dữ liệu cho Tỉnh, việc đầu tư các hạ tầng và thiết bị tách biệt (siloes) với nhau về lâu dài sẽ tạo ra thách thức về khả năng mở rộng và quản trị. Để đảm bảo trách độ phức tạp về lâu dài, nên có định hướng chuyển sang việc đầu tư các hệ thống hạ tầng hội tụ hoặc tích hợp ngay từ đầu.

<u>Kiến trúc hạ tầng IoT Đô thị thông minh</u>

Ngoài ra, như ở trên đã đề cập, việc xây dựng riêng một kiến trúc cho hạ tầng IoT cũng là một vấn đề cần thiết trong việc xây dựng kiến trúc hạ tầng nói riêng hay kiến trúc CQĐT nói chung của Tỉnh. Kiến trúc hạ tầng IoT phải được chuẩn hóa và hoạch định để phù hợp với các lĩnh vực (ngành) sẽ sử dụng phổ biến các hệ thống cảm biến IoT trong tương lai như Giao thông, Môi trường, Y tế... phù hợp và hỗ trợ tốt các dịch vụ nền tảng của Cách mạng công nghiệp 4.0 như AI, Machine Learning. Để bảo đảm đáp ứng được các yêu cầu của ĐTTM, hạ tầng IoT cần phải được xem xét, thiết kế một cách tổng thể, xuyên suốt từ ứng dụng cho đến hạ tầng kỹ thuật. Hai hình vẽ sau mô tả khái quát Kiến trúc hạ tầng IoT theo hai phương diện: ứng dụng và kỹ thuật.

Hạ tầng về IoT cơ bản gồm có 03 khối chính:

(1) Hạ tầng cảm biến: Cung cấp khả năng theo dõi và quản lý các thiết bị cảm biến (sensors), điều khiển (controllers). Đây chính là nơi thu thập dữ liệu, thông tin từ các thiết bị phục vụ cho đô thị thông minh trong các lĩnh vực như: Giao thông, y tế, môi trường... như đã mô tả trong phần kiến trúc ứng dụng IoT. Đây cũng chính là nơi cung cấp khả năng điều khiển, tương tác giữa các thiết bị điều khiển, hạ tầng đô thị... Trong thực tế, đây sẽ là một phần hạ tầng cực kỳ thách thức vì

sự đa dạng về công nghệ, tiêu chuẩn trong điều khiển, truyền dữ liệu... Vì thế ngay từ đầu, Tỉnh cần đưa ra các tiêu chuẩn dựa tên các tiêu chuẩn quốc tế để tránh các phát sinh và độ phức tạp về sau trong quá trình tích hợp.

(2) Mạng cảm biến:

- Cung cấp khả năng kết nối, tương tác giữa các thiết bị cảm biến, điều khiển với các cơ sở dữ liệu phân tán, tập trung hoặc các nguồn thông tin và công cụ quản lý khác.

- Mạng cảm biến sẽ dựa trên hạ tầng mạng diện rộng và mạng viễn thông, cung cấp khả năng truyền dữ liệu, thông tin liên lạc (một chiều hoặc hai chiều), phát hiện (discovery) các thiết bị trong hạ tầng cảm biến.

- Hầu hết các nhu cầu sử dụng sẽ không quá lớn, tuy nhiên trong một số trường hợp đặc thù như: Phân tích video, ra quyết định điều khiển giao thông sẽ cần băng thông lớn và độ trễ nhỏ. Vì thế việc đầu tư hạ tầng mạng diện rộng và hạ tầng viễn thông, từ đó cung cấp khả năng cho hạ tầng mạng cảm biến là hết sức quan trọng trong việc xây dựng CQĐT và Đô thị thông minh.

(3) Hạ tầng tính toán, xử lý biên (Edge computing)

- Cung cấp khả năng tự động hóa và ra quyết định ở gần với môi trường được theo dõi, giúp giảm thiểu độ trễ và giảm rủi ro trong việc mất điều khiển toàn bộ hệ thống hạ tầng IoT.

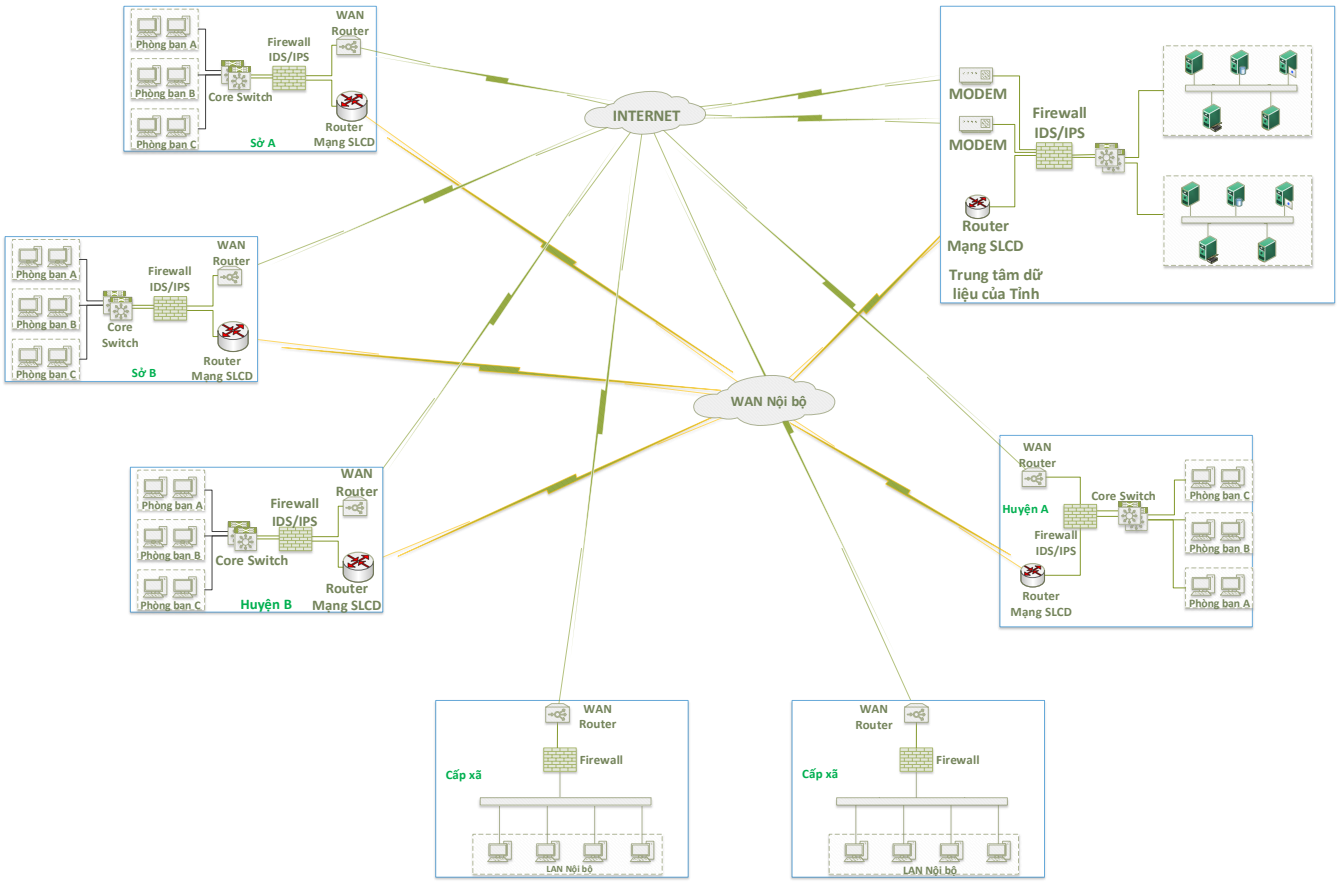
- Việc thu thập thông tin, ra quyết định và có hành động tương tác hoặc điều khiển cũng như truyền thông (communicate) giữa các thiết bị tạo thành hạ tầng IoT là rất quan trọng. Trong một số trường hợp cần độ trễ rất thấp nhằm đảm bảm an toàn về tài sản và tính mạng. Từ đó việc tập trung toàn bộ năng lực xử lý và ra quyết định trong các trung tâm dữ liệu đôi khi sẽ không đáp ứng được.

- Việc xây dựng hạ tầng tính toán, xử lý biên sẽ phụ thuộc rất lớn vào nhu cầu từ các ngành đặc thù, chưa kể đến các thách thức khác về mặt quản trị, cấp phát, đảm bảo an toàn và tuân thủ.

2.3. Xác định các mô hình mạng và nền tảng mạng truyền thông

2.3.1 Xác định mô hình mạng tổng thể (nội bộ và kết nối ra bên ngoài của tỉnh)

Mô hình kết nối mạng tổng thể của tỉnh Bình Phước được thiết kế trên cơ sở tách biệt đường WAN với đường truyền internet để đảm bảo sự bảo mật và an toàn dữ liệu từ cấp huyện đến cấp tỉnh và dữ liệu truyền về Trung tâm dữ liệu tỉnh luôn ổn định. Ngoài ra, chúng tôi đề xuất xây dựng mô hình cho từng đơn vị đồng bộ thống nhất đảm bảo cho việc vận hành được tối ưu với các thiết bị được đầu tư mới, dự kiến sẽ thay thế dần các thiết bị cũ, lạc hậu hoặc hết khấu hao sử dụng trong thời gian từ năm 2018-2020, định hướng 2025. Mô hình kiến trúc mạng tổng thể cho toàn tỉnh Bình Phước được đề xuất như sau

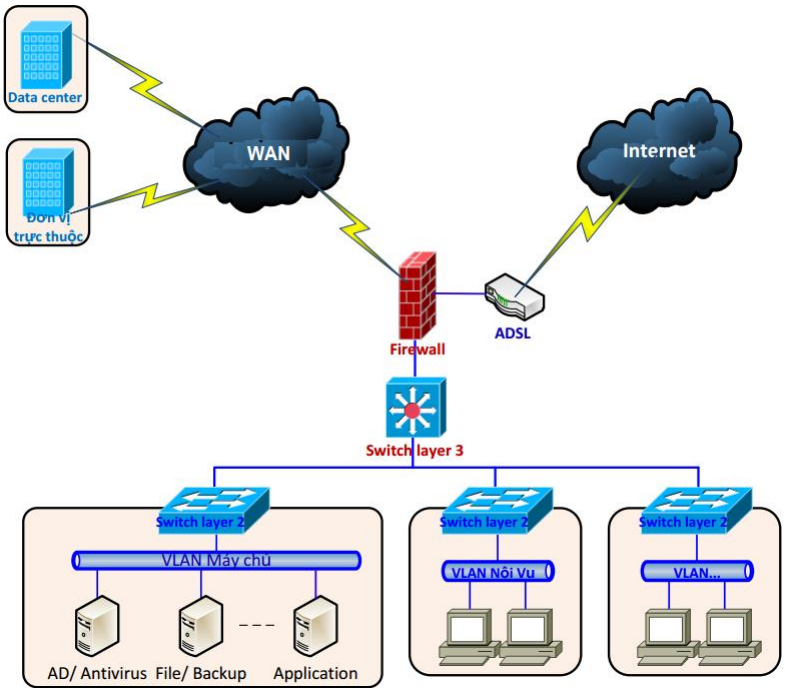


Mô hình kết nối mạng tổng thể

Các kết nối WAN có thể hoặc được dành riêng các đường dây mạng WAN hoặc chạy các VPN tunnel trong kết nối Internet, sử dụng IPsec. Để hình thành mạng WAN, tỉnh tận dụng tối đa hệ thống mạng LAN sẵn có của các đơn vị trên cơ sở tiến hành đầu tư hoàn chỉnh hệ thống mạng tại các cơ quan hành chính trên địa bàn tỉnh theo mô hình mạng điển hình chuẩn cho các cấp, tiến tới kết nối hệ thống mạng riêng lẻ vào mạng WAN chung của tỉnh, hình thành mạng WAN chung, thống nhất cho toàn tỉnh.

2.3.2 Xác định mô hình mạng điển hình của 1 cơ quan (LAN), sơ đồ kết nối với mạng chung của Tỉnh

a) Mô hình mạng điển hình tại các Sở, ban, ngành và các đơn vị cấp Huyện:



Mô hình mạng điển hành tại các Sở, ban, ngành và các đơn vị cấp Huyện

- Kết nối về Trung tâm dữ liệu của Tỉnh:

Để đảm bảo kết nối về TTDL của tỉnh được thông suốt và an toàn thì tại các đơn vị cấp Huyện và các Sở, ban, ngành ngoài việc trang bị đường WAN để kết nối vào mạng nội bộ chung của Tỉnh, cần phải có một đường kết nối dự phòng thay thế khi đường WAN gặp sự cố nhưng phải đảm bảo an toàn, bảo mật.

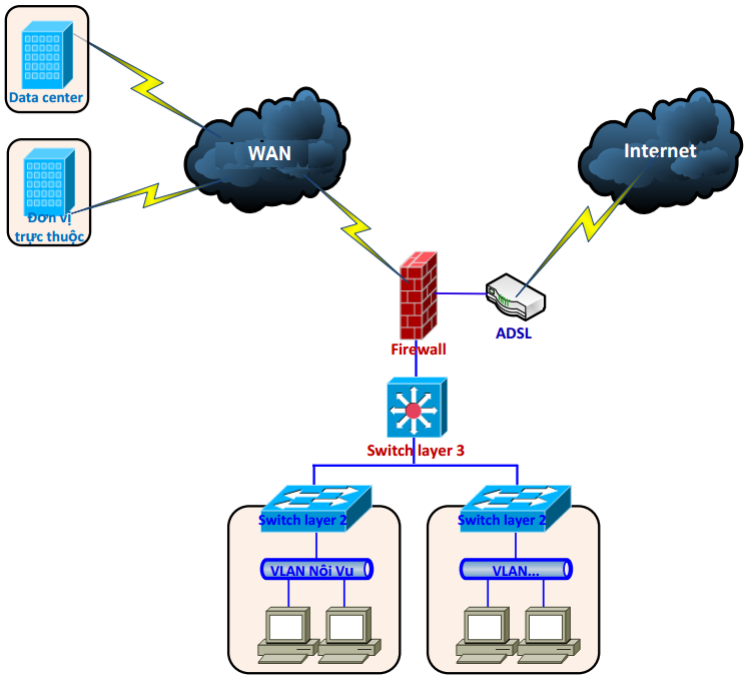
Giải pháp xây dựng đường kết nối dự phòng được đề xuất là tạo thêm các kết nối VPN site - to - site từ các đơn vị cấp Huyện và Sở, ban, ngành về TTDL của tỉnh để làm kết nối dự phòng. Kết nối VPN site-to-site được tạo và thiết lập hoạt động ở chế độ dự phòng, khi đường WAN (đường truyền chính kết nối về TTDL) gặp sự cố thì đường kết nối VPN site-to-site sẽ chuyển sang chế độ chạy chính cho đến khi đường WAN được khôi phục, nó sẽ chuyển về chế độ hoạt động dự phòng và đường WAN sẽ trở lại chạy chính. Để làm được điều này thì tại TTDL phải trang bị và xây dựng 1 hệ thống VPN server để chấp nhận các kết nối VPN site-to-site từ các đơn vị thông qua Internet và các đơn vị cần có thiết bị router hoặc tường lửa có hỗ trợ VPN site-to-site để tạo kết nối VPN về TTDL.

Trung tâm dữ liệu của tỉnh sẽ đầu tư hệ thống thiết bị VPN Server để quản lý các kết nối VPN tại các đơn vị tập trung về Trung tâm dữ liệu. Do đó việc tạo các kết nối VPN sẽ được thay thế bằng cách thiết lập thông qua các WAN Router được đầu tư mới trong giai đoạn này nhằm dự phòng cho đường WAN với bộ phần mềm quản trị tập trung tổng thể các thiết bị tại Trung tâm tích hợp dữ liệu có khả năng cấu hình từ xa thông qua nhiều hình thức khác nhau như: Telnet, SSH… và có khả năng theo dõi giám sát để kịp thời đánh giá đưa ra phương án khắc phục sự cố.

- Kết nối Internet: Chúng tôi khuyến nghị các đơn vị cấp Huyện và các Sở, ban, ngành cần trang bị ít nhất hai đường truyền internet cáp quang. Mục đích chính là để đảm bảo kết nối VPN

luôn luôn được duy trì khi một trong 02 đường truyền internet gặp sự cố đồng thời cung cấp truy cập internet ổn định cho người dùng phục vụ công việc nội bộ.

b) Mô hình mạng điển hành tại cấp Xã:



Mô hình mạng điển hành tại cấp Xã

- Kết nối sử dụng các dịch vụ dùng chung: Để đảm bảo có thể truy cập vào các dịch vụ nội bộ dùng chung của tỉnh được thông suốt và an toàn thì tại đơn vị cấp Xã thì trong tương lai chúng tôi đề xuất mở rộng trang bị đường WAN.

Trong điều kiện hiện tại, để thể truy cập vào các dịch vụ nội bộ dùng chung của tỉnh, các đơn vị cấp Xã được khuyến nghị sử dụng các kết nối VPN site-to-site để kết nối về huyện thông qua đường truyền internet cáp quang. Các đơn vị cần có thiết bị router hoặc tường lửa có hỗ trợ VPN site-to-site để tạo kết nối VPN về huyện.

- Kết nối Internet: Chúng tôi khuyến nghị các đơn vị cấp Xã cũng cần trang bị ít nhất 02 đường truyền internet cáp quang để kết nối VPN về huyện hoặc Trung tâm dữ liệu và cung cấp truy cập internet ổn định cho người dùng phục vụ công việc

2.3.3 Các nền tảng công nghệ mạng truyền dẫn

Các nền tảng Mạng là những công nghệ được sử dụng để đơn giản hóa quá trình truyền tải mạng thông tin giữa các thành phần ứng dụng và người dùng.

- Mạng giao dịch (Delivery Network): Mạng giao dịch là loại hình mạng được sử dụng để chuyển giao các ứng dụng và/ hoặc thông tin tới người dùng. Một số mạng giao dịch phổ biến hiện nay gồm có:

  - Internet: là hệ thống mạng máy tính toàn cầu mà người dùng tại bất kỳ máy tính nào, nếu có quyền, đều có thể lấy thông tin từ bất cứ một máy tính khác.
  - Intranet: là hệ thống mạng riêng trong tỉnh, có thể bao gồm nhiều mạng cục bộ (LAN)

kết nối với nhau và được dùng để chia sẻ thông tin cũng như tài nguyên của cơ quan, đơn vị, tỉnh giữa các cán bộ.

- Extranet: là hệ thống mạng riêng sử dụng giao thức Internet và hệ thống viễn thông công cộng để chia sẻ an toàn một phần thông tin trong tỉnh hoặc các hoạt động với các nhà cung cấp, liên doanh, đối tác, khách hàng hoặc các cơ quan, đơn vị khác. Mạng extranet có thể được xem như một phần của mạng intranet trong tỉnh nhưng được mở rộng với người dùng bên ngoài phạm vi quản lý của tỉnh.
- Mạng riêng Ảo (Virtual Private Network - VPN): VPN tận dụng cơ sở hạ tầng viễn thông công cộng duy trì tính bảo mật thông qua việc sử dụng giao thức tạo đường hầm (tunneling protocol) và các thủ tục bảo mật (security procedures).

- Chuyển tải mạng: Chuyển tải mạng là các phương tiện chức năng và thủ tục chuyển tải các chuỗi dữ liệu với độ dài biến đổi từ một máy chủ nguồn trên hệ thống mạng này đến một máy chủ đích trên hệ thống mạng khác, nhưng vẫn đảm bảo được chất lượng của dịch vụ. Một số giải pháp chuyển tải mạng phổ biến gồm có:

- IP (Internet Protocol): là giao thức chính trong Tầng Internet (Internet Layer) của Bộ Giao thức Internet (Internet Protocol Suite) và có nhiệm vụ chuyển giao các gói dữ liệu (datagrams) từ máy chủ nguồn đến máy chủ đích hoàn toàn dựa trên địa chỉ của các gói dữ liệu này. Với mục đích này, IP xác định các phương pháp và cấu trúc ghi địa chỉ để đóng gói các gói dữ liệu.
- Internetwork Packet Exchange (IPX): là giao thức tầng mạng mô hình OSI (OSI-model Network layer protocol) trong chồng giao thức IPX/SPX. Nhìn chung, việc sử dụng IPX đã giảm do sự bùng nổ của Internet đã làm TCP/IP gần như phổ biến trên toàn cầu. Máy tính và các hệ thống mạng có thể vận hành nhiều giao thức mạng, do đó, hầu như tất cả các điểm IPX sẽ chạy TCP/IP và cho phép kết nối Internet.

- Chuyển tải ứng dụng: Chuyển tải ứng dụng bao gồm tất cả các giao thức và phương thức thuộc lĩnh vực trao đổi thông tin giữa các quy trình (process-to-process communications) trong hệ thống mạng. Các phương thức chuyển tải ứng dụng sử dụng các giao thức tầng chuyển tải cơ sở để thiết lập kết nối giữa các máy chủ (host-to-host connections). Một số giải pháp về chuyển tải ứng dụng:

- FTP (file transfer protocol - Giao thức truyền tập tin): là một chuẩn giao thức mạng sử dụng để truyền tập tin từ máy chủ này đến một máy chủ khác thông qua một mạng lưới có nền TCP, ví dụ như mạng Internet. FTP được phát triển trên kiến trúc khách-chủ, tận dụng kiểm soát riêng và kết nối dữ liệu giữa máy chủ và máy khách. Người dùng FTP có thể tự xác thực bằng cách sử dụng giao thức đăng nhập ở dạng văn bản thường (clear-text sign-in protocol) nhưng có thể kết nối ẩn danh nếu máy chủ cho phép.
- SMTP (simple mail transfer protocol - giao thức truyền tải thư tín đơn giản): là một chuẩn Internet truyền tải thư điện tử (e-mail) qua mạng Giao thức Internet (IP). SMTP bao gồm SMTP mở rộng (ESMTP), và là giao thức được dùng phổ biến hiện nay.
- HTTP (hypertext transfer protocol - giao thức truyền tải siêu văn bản): là một giao thức

mạng cho các hệ thống thông tin phân phối, hợp tác, siêu phương tiện. HTTP là cơ sở trao đổi dữ liệu cho World Wide Web (WWW).

- Các giao diện vật lý và kết nối: Các giao diện vật lý và kết nối là giao thức trao đổi thông tin cung cấp cơ chế kiểm soát ghi địa chỉ và truy cập kênh cho phép các thiết bị đầu cuối và các nút mạng có thể trao đổi thông tin trong một mạng đa điểm. Một số giao diện vật lý và kết nối:

  - Ethernet: tầng vật lý Ethernet đã phát triển qua một khoảng thời gian đáng kể và gồm nhiều giao diện truyền thông vật lý, dung lượng truyền khác nhau. Tốc độ thường dao động từ 1 Mbit/s đến 100 Gbit/s trong khi đó phương tiện vật lý phát triển từ cáp đồng trục, cáp xoắn, tới cáp quang. Nhìn chung, phần mềm chồng giao thức mạng sẽ hoạt động tương tự nhau trong tất cả các tầng vật lý.
  - IEEE 802.11: là tập hợp các chuẩn thực hiện trao đổi thông tin trên máy tính trong mạng cục bộ không dây (WLAN), băng tần tần số 2.4, 3.6, và 5 GHz. Các băng tần tần số này được tạo ra và duy trì bởi IEEE LAN/MAN Standards Committee (IEEE 802). Phiên bản hiện tại của chuẩn này là IEEE 802.11-2007. Các chuẩn này cung cấp cơ sở cho mạng không dây Wi-Fi.
  - Giao diện Dữ liệu Phân bố theo Cáp sợi quang (Fiber Distributed Data Interface-FDDI): cung cấp chuẩn quang truyền tải dữ liệu trong mạng cục bộ với tốc độ 100 Mbit/s và có thể hoạt động trong khu vực 200km (124 dặm). Mặc dù cấu trúc topo lôgíc FDDI là mạng vòng chuyển thẻ bài, nhưng cấu trúc này không sử dụng giao thức vòng chuyển thẻ bài IEEE 802.5 như nền tảng của mình; thay vào đó, giao thức của FDDI bắt nguồn từ giao thức thẻ bài với mạng BUS IEEE 802.4.

- Các dịch vụ mạng hỗ trợ: Các dịch vụ mạng hỗ trợ là các giao thức hỗ trợ được sử dụng để trợ giúp việc quản lý mạng. Một số dịch vụ mạng hỗ trợ:

  - DNS (domain name system - Hệ thống tên miền): là hệ thống đặt tên theo thứ tự được phát triển trên cơ sở dữ liệu phân tán cho máy vi tính, dịch vụ, hoặc bất kì nguồn nào kết nối với Internet hoặc một mạng riêng. Quan trọng nhất là, DNS chuyển tên miền có ý nghĩa đối với con người vào số định danh (nhị phân), liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị này khắp thế giới.
  - DHCP (dynamic host configuration protocol - Giao thức cấu hình động máy chủ): là giao thức cấu hình tự động được sử dụng trên hệ thống mạng IP. Máy tính kết nối vào mạng IP phải được cấu hình trước khi trao đổi thông tin với các máy tính khác trong hệ thống mạng. DHCP cho phép một máy tính được cấu hình một cách tự động vì thế sẽ giảm việc can thiệp của người quản trị vào hệ thống mạng. DHCP cũng cung cấp một cơ sở dữ liệu trung tâm để theo dõi tất cả các máy tính kết nối vào hệ thống mạng nhằm tránh trường hợp hai máy tính khác nhau lại có cùng địa chỉ IP.

2.4. Xác định mô hình triển khai Trung tâm dữ liệu

2.4.1 Các yêu cầu cơ bản về Trung tâm dữ liệu

Trong tương lai, tỉnh Bình Phước cần tiếp tục hoàn thiện Trung tâm dữ liệu hiện đại của Tỉnh, đáp ứng yêu cầu đầu tư mới và mở rộng, nâng cấp các hệ thống CNTT, CSDL, trong đó có

các hệ thống chính quyền điện tử. Trung tâm dữ liệu của tỉnh trong tương lai cần đáp ứng các yêu cầu cơ bản sau:

- Có hạ tầng hiện đại theo tiêu chuẩn quốc tế.

- Có kiến trúc mạng và bảo mật đảm bảo phục vụ các kết nối an toàn đến các hệ thống thông tin tại Trung tâm.

- Trung tâm dữ liệu được đặt tại vị trí an toàn, đảm bảo tránh được bão, lụt và các thảm họa thiên nhiên khác.

- Trung tâm được đặt tại địa điểm được bảo vệ an toàn.

- Có diện tích đáp ứng yêu cầu của các hệ thống hiện tại cũng như khả năng mở rộng trong tương lai.

- Có đường giao thông thuận tiện, đáp ứng yêu cầu vận chuyển thiết bị, nhiên liệu phục vụ hoạt động của trung tâm.

- Được cung cấp nguồn điện ổn định từ lưới điện quốc gia.

- Có kết nối đến các nhà cung cấp viễn thông khác nhau, đảm bảo các kết nối WAN và Internet với chất lượng ổn định, băng thông đáp ứng yêu cầu.

- Trung tâm được thiết kế đáp ứng tiêu chuẩn Tier 3 về Datacenter.

- Có hệ thống sàn nâng, máng cáp theo tiêu chuẩn. Có hệ thống vách ngăn chống cháy và cửa cường lực đảm bảo an toàn cho trung tâm cũng như cho nhân viên vận hành.

- Có hệ thống máy phát điện riêng đảm bảo hoạt động khi có sự cố về điện lưới. Hệ thống bồn chứa nhiên liệu đảm bảo trung tâm có thể hoạt động tối thiểu 24h khi có sự cố điện lưới.

- Có hệ thống UPS công suất lớn, hoạt động theo chế độ online, được thiết kế theo tiêu chuẩn N+1, đảm bảo hệ thống luôn vận hành liên tục, ổn định không bị ngắt quãng.

- Có hệ thống điều hòa chuyên dụngcho trung tâm dữ liệu, đảm bảo môi trường hoạt động theo tiêu chuẩn cho các hệ thống máy móc, thiết bị CNTT.

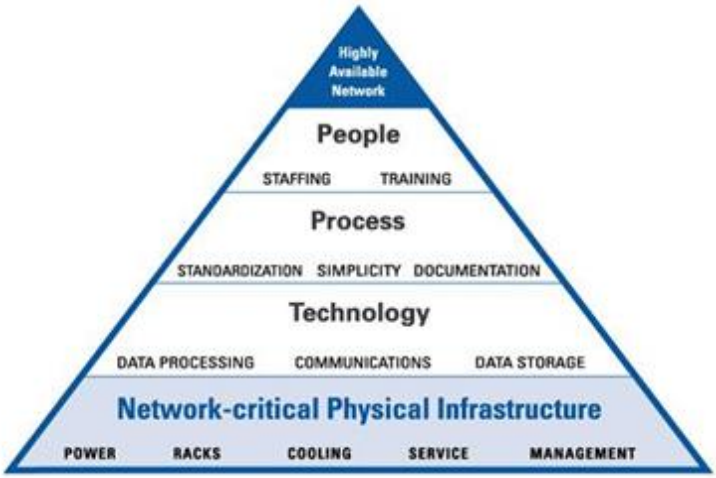
- Có hệ thống giám sát hoạt động, hệ thống cảnh báo cháy nổ, rò rỉ nước...

- Có hệ thống phòng chống cháy chuyên dụng cho trung tâm dữ liệu, đảm bảo các yêu cầu về phòng chống cháy nổ.

- Có hệ thống camera giám sát, hệ thống an toàn bảo mật hệ thống.

2.4.2 Mô hình triển khai hạ tầng vận hành TTDL

Hiện nay, Trung tâm dữ liệu tỉnh Bình Phước đã được thiết kế trên cơ sở đáp ứng phần lớn các tiêu chuẩn quốc tế về Tier 2. Tuy nhiên, với sự gia tăng số lượng, quy mô hệ thống CNTT trong tương lai thì Trung tâm dữ liệu của tỉnh sẽ cần sẵn sàng đáp ứng các yêu cầu mới về cơ sở vật lý hạ tầng thiết yếu-NCPI (Network- Critical Physical Infrastructure) để đảm bảo an toàn hoạt động, vận hành của hệ thống. Vì vậy, chúng tôi khuyến nghị xem xét tái cấu trúc các thành phần của TTDL thành các khối chuẩn, mở và có khả năng mở rộng. Mô hình của NCPI như sau:



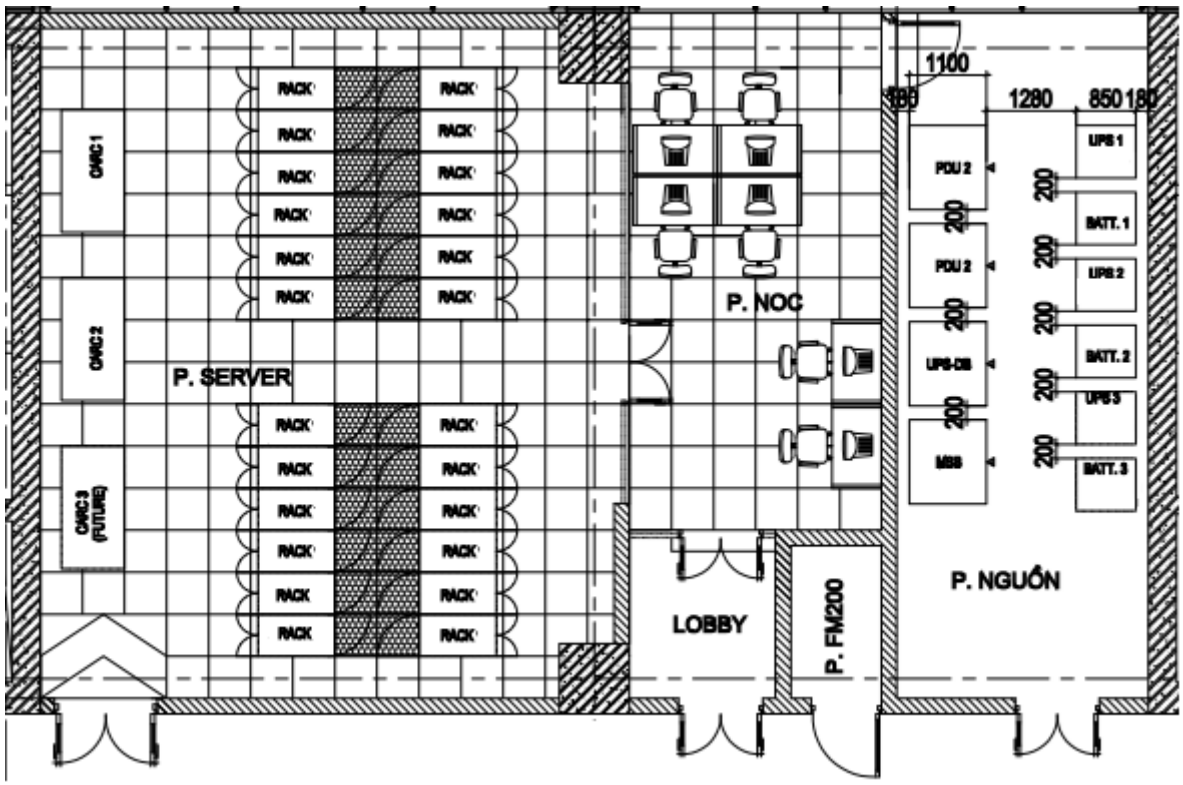
Mô hình của Mạng hạ tầng vật lý thiết yếu

Mô hình NCPI bao gồm:

- Hệ thống nguồn điện;
- Hệ thống UPS;
- Hệ thống phân phối nguồn;
- Hệ thống máy phát điện;
- Tủ Rack;
- Hệ thống làm mát;
- Hệ thống cáp mạng;
- Hệ thống truyền thông;
- Hệ thống quản trị;
- Hệ thống báo động, đo nhiệt độ môi trường và báo cháy báo nổ, PCCC;
- Hệ thống dịch vụ…

Ngoài ra, Trung tâm dữ liệu cũng phải đảm bảo bố trí không gian hành lang: dùng để đi lại và vận chuyển thiết bị phục vụ TTDL.

TTDL của tỉnh Bình Phước được khuyến nghị gồm các phòng chức năng độc lập với nhau về mặt vật lý:



Mô hình thiết kế tham chiếu mặt bằng TTDL

- Phòng máy chủ, thiết bị mạng (SR room): Chỉ dành để bố trí các thiết bị CNTT và hệ thống làm mát kiểu thổi sàn riêng cho các TB CNTT. Để dảm bảo an ninh thì muốn vào được phòng SR bắt buộc phải đi qua NOC. Cửa riêng của phòng SR ra hành lang chỉ mở để phục vụ trường hợp vận chuyển thiết bị

- Phòng cơ điện (M&E): Để bố trí các thiết bị tủ điện, thiết bị lưu điện UPS, acquy, chống sét... (nói chung gồm các thiết bị phân phối bảo vệ điện áp cho TTDL). Hệ thống điện cần kiểm tra thường xuyên bởi nhân viên chuyên trách, cần trang bị hệ khóa từ để đảm bảo an ninh.

- Phòng trực giám sát vận hành (NOC): Dành cho nhân viên vận hành hệ thống mạng, giám sát hoạt động của TTDL. Phòng này được bố trí ở giữa P.SR và P.M&E dể thuận tiện cho việc giám sát vận hành.

- Phòng đệm (Lobby): Trước khi vào được NOC thì bắt buộc phải đi qua lobby. Phòng này nhăm mục đích tăng thêm một tầng cửa an ninh, cũng là nơi người vào phải bỏ lại các trang phục hoặc vật dụng không phù hợp trước khi vào bên trong khu vực làm việc.

- Phòng đặt bình khí chữa cháy (Fire Cylind): Dành riêng bố trí các bình khí chữa cháy, có cửa riêng thường khóa kín. Việc tách riêng các bình chữa cháy để tăng mỹ quan và đảm bảo an toàn, chống can thiệp vô ý vào bình làm xả khí gây uy hiếp đến đảm bảo an toàn cháy nổ trong TTDL.

- Sau đây là một số tiêu chí cần đáp ứng đối với các thành phần hạ tầng vận hành TTDL:

STT	Thành phần hệ thống	Yêu cầu
1	Hệ thống phân phối điện Trạm biến áp Máy phát điện + ATS Tủ điện phân phối Dây cáp điện	Cung cấp nguồn dự phòng khi xảy ra sự cố mất điện lưới ≥ 36h. Đảm bảo cung cấp liên tục 24 giờ/ ngày, 365 ngày/năm
2	Hệ thống UPS online	Dự phòng cung cấp điện 15 phút Chế độ dự phòng (N+1) Công nghệ parallel
3	Hệ thống làm mát bằng điều hòa chính xác	Đảm bảo cung cấp liên tục 24 giờ/ngày, 365 ngày/năm Tự điều chỉnh nhiệt độ và độ ẩm Giải pháp thổi sàn Chế độ dự phòng (N+1)
4	Hệ thống an ninh giám sát Access control Camera IP	Giám sát toàn bộ Phòng máy chủ Lưu dữ liệu tối thiểu 30 ngày Kiểm soát truy cập ra vào các phòng chức năng trong TTDL bằng vân tay hoặc mã code
5	Hệ thống phát hiện rò rỉ chất lỏng	Giám sát và cảnh báo chất lỏng
6	Hệ thống quản trị tập trung và màn hình giám sát	Giám sát UPS. Điều hòa chính xác, Máy phát, hệ thống giám sát môi trường, FM200, Access control. Cảnh báo bằng SMS, mail. Màn hình giám sát sử dụng màn hình 46inch
7	Hệ thống sàn nâng (phòng Server, phòng M&E)	Chiều cao sàn nâng phòng máy chủ 500mm Sàn trơn làm cho phòng NOC và phòng Lobby chiều cao 200mm
8	Hệ thống chiếu sáng và chiếu sáng khẩn cấp	Chiều sáng khẩn cấp và chiếu sáng làm việc lắp cho tất cả các khu vực trong Phòng máy chủ.
9	Hệ thống tủ rack	Tủ rack Network dùng loại có chiều rộng 800mm, chiều sâu tối thiểu là 1090mm Tủ rack Server dùng loại có chiều rộng 600mm, chiều sâu tối thiểu là 1090mm

STT	Thành phần hệ thống	Yêu cầu
10	Hệ thống phòng cháy chữa cháy	Dùng hệ thống PCCC bảo vệ cho phòng SR, phòng M&E, bảo vệ cả trên và dưới sàn nâng.
11	Hệ thống vách ngăn, cửa chống cháy, trần thả. Thang máng cáp	Sử dụng trần thạch cao kích thước (600x600) mm Máng cáp mạng sử dụng máng cáp cablofil Thang máng cáp điện sử dụng loại máng thép sơn tĩnh điện Vách kính cường lực 12mm, vách tường kháng cháy
12	Hệ thống cấu trúc cáp	Sử dụng giải pháp 3 cross connect
13	Hệ thống tiếp địa và cắt lọc sét	2 đường tiếp địa (1 cho lọc sét, 1 cho nối đất an toàn vỏ thiết bị) Hệ thống cắt lọc sét (sơ cấp và thứ cấp)
14	Thiết bị phòng NOC	Trang bị bàn ghế, laptop, máy in, …
15	Xây dựng cơ bản	Khả năng chịu cháy tối thiểu 1h, vách ngăn có khả năng chống bám bụi tốt…

2.4.3 Mô hình triển khai hạ tầng CNTT tại TTDL

a) Mô tả chung về hạ tầng Trung tâm dữ liệu tỉnh

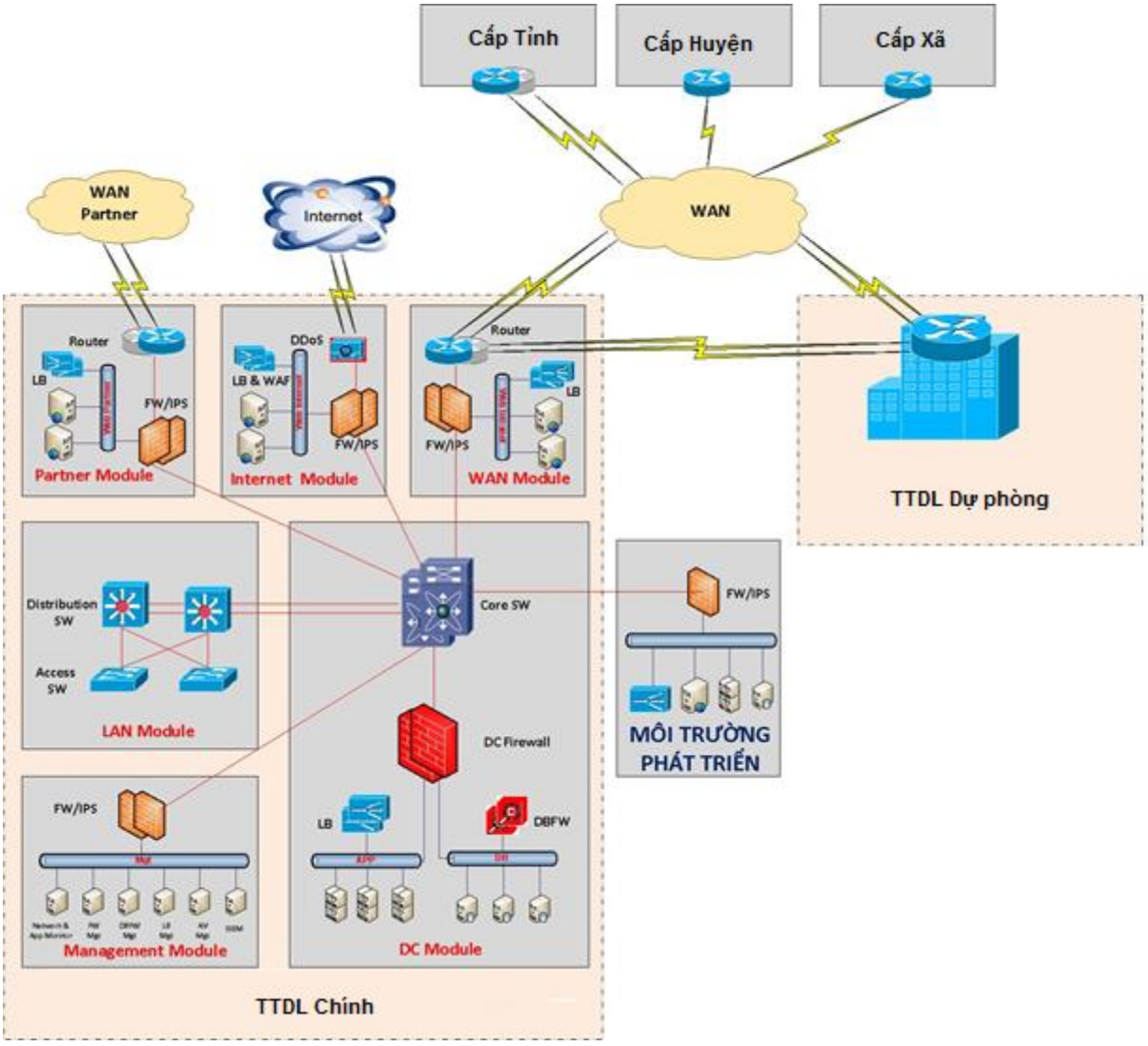
Trung tâm dữ liệu của tỉnh là nơi lưu trữ, xử lý khối lượng dữ liệu lớn của các lĩnh vực trong tỉnh, cung cấp các dịch vụ, ứng dụng quan trọng của tỉnh, trong đó dịch vụ công trực tuyến của tỉnh cơ bản được triển khai, vận hành tại đây. Do đó, các Trung tâm dữ liệu là nơi tập trung năng lực tính toán mạnh mẽ, có các kết nối mạng tốc độ cao, ổn định, đảm bảo an ninh, bảo mật và phòng chống cháy nổ, khả năng dự phòng ở mức cao. Tuy nhiên, hiện nay, tỉnh Bình Phước chưa có Trung tâm dữ liệu, các hệ thống chỉ được triển khai trên phòng máy chủ chưa đủ tiêu chuẩn của tỉnh. Đồng thời, hạ tầng kỹ thuật CNTT tại TTDL của tỉnh hiện này tồn tại nhiều điểm đơn có thể gây chết hệ thống, chưa đảm bảo tính an toàn về mặt dự phòng.

b) Mô hình triển khai nâng cấp, mở rộng TTDL

Để giải quyết hiện trạng hiện nay, tỉnh Bình Phước cần xây dựng Trung tâm dữ liệu của tỉnh và nâng cấp toàn diện hạ tầng kỹ thuật CNTT của tỉnh để sẵn sàng tiếp nhận các kết nối từ các cơ quan, đơn vị hành chính trên địa bàn tỉnh kết nối đến Trung tâm dữ liệu vì xu thế tập trung ứng dụng, tập trung dữ liệu sẽ là tất yếu. Tỉnh cần đầu tư nâng cao năng lực của hệ thống máy chủ tính toán, tăng cường năng lực đảm bảo an toàn, bảo mật, an ninh thông tin cho các hệ thống của TTDL (DDOS, Load Balancing và Tường lửa vùng Database, hệ thống SIEM, hệ thống NOC, NPM...), giải quyết triệt để các điểm chết đơn của hệ thống bằng cách bổ sung thiết bị chạy HA cho các thiết

bị đang chạy đơn. Ngoài ra, các hệ thống máy chủ còn tồn tại bên ngoài TTDL của các đơn vị hành chính cần được xem xét để chuyển đổi dần về Trung tâm dữ liệu của tỉnh trong tương lai. Một trong việc quan trọng cần phải làm là

Sơ đồ thiết kế tổng thể Trung tâm dữ liệu tỉnh Bình Phước khuyến nghị tham chiếu như sau:



- TTDL của tỉnh Bình Phước cần phải được thiết kế để đảm bảo tính sẵn sàng cao nhất và năng lực thực thi phục vụ các hệ thống ứng dụng nghiệp vụ và CSDL của tỉnh sẽ bao gồm: TTDL Chính và TTDL Dự phòng. Thiết kế sơ bộ cho DC (DR có mô hình tương tự DC nhưng công suất có thể sẽ được tính toán thấp hơn DC) được dựa trên phương pháp thiết kế phân lớp (Hierarchical) và và mô-đun (Modular).

+ Trung tâm dữ liệu chính (DC): Nơi tập trung toàn bộ hạ tầng CNTT phục vụ cho các ứng dụng của tỉnh do Sở TTTT quản lý. TTDL được đầu tư trang thiết bị với công nghệ tiên tiến phù hợp với việc triển khai các ứng dụng, khai thác dịch vụ mạng đến năm 2020. Đây là TTDL mới của tỉnh kết nối với Trung tâm dữ liệu dự phòng (DR) nhằm đảm bảo an toàn dữ liệu cũng như khôi phục dữ liêu khi có sự cố xảy ra.

+ Trung tâm dữ liệu dự phòng (DR): Thực hiện chức năng dự phòng cho hoạt động tại

TTDL chính. TTDL hiện cần phải được được đầu tư nâng cấp để thành TTDL dự phòng trong giai đoạn sau khi đã hoàn thành Trung tâm dữ liệu chính. TTDL chính (DC) và TTDL dự phòng (DR) được kết nối với nhau thông qua các kết nối SAN FC-to-SAN FC trực tiếp hoặc thông qua kết IP phục vụ việc đồng bộ dữ liệu giữa DC và DR.

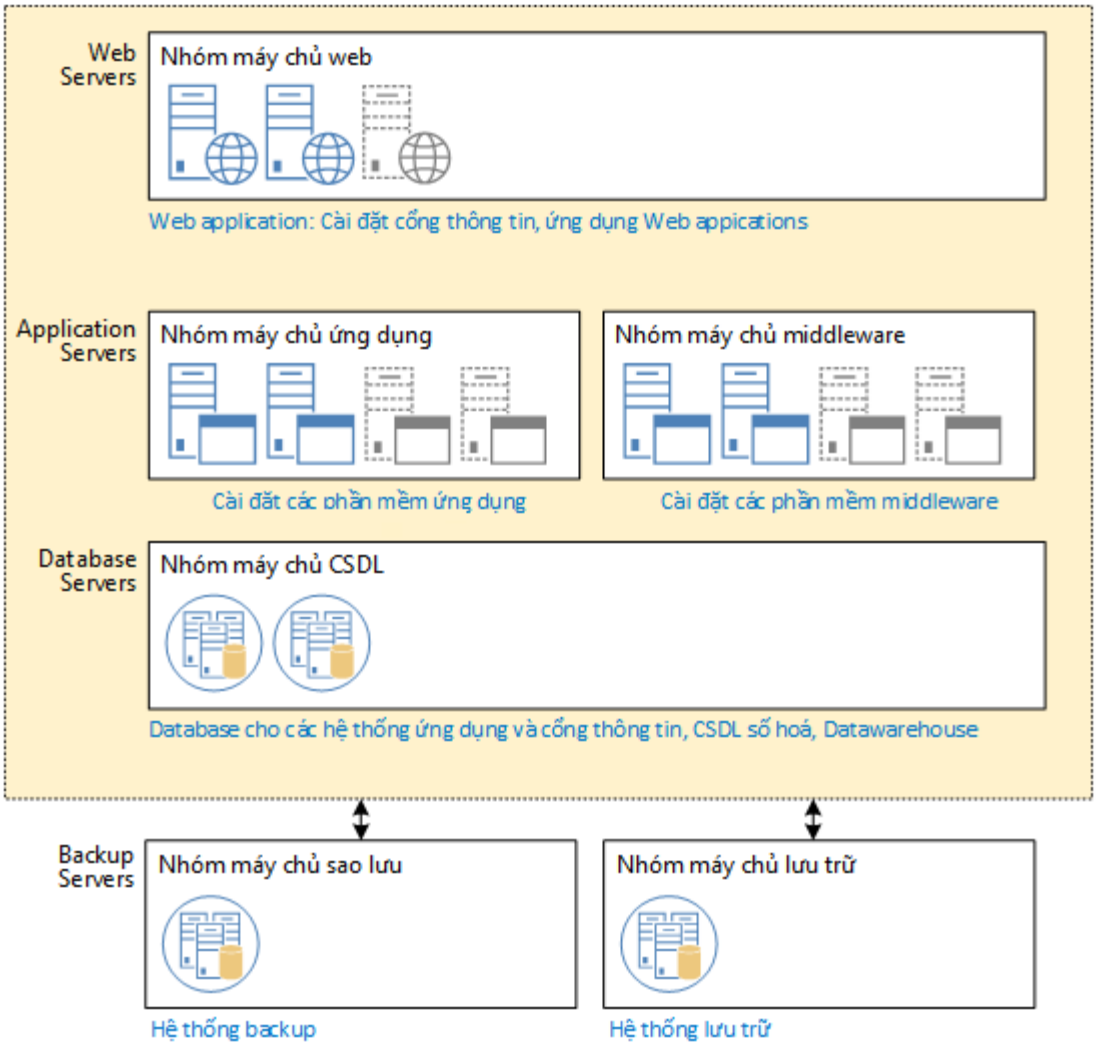
- Mô hình mạng trong TTDL được thiết kế theo mô hình Leaf-spine với Core switch đóng vai trò Spine và các switch/blade switch đóng vai trò Leaf.

- TTDL của tỉnh sẽ bao gồm các thành phần:

+ Data Center Module: Là thành phần quan trọng nhất trong TTDL, đặt toàn bộ các hệ thống máy chủ và CSDL của toàn tỉnh. Module bao gồm các thiết bị Core Switch giữ vai trò định tuyến và chuyển tiếp lưu thông giữa các phân hệ, đảm bảo cung cấp các kết nối với tốc độ 01/10/40 Gbps cho các Server, các thiết bị chuyên dụng như Firewall, thiết bị cân bằng , tường lửa CSDL...

Vùng Server Farm được thiết kế theo mô hình Muti-tier: Aplication, Database mỗi vùng vùng muốn truy cập tới nhau phải thông qua thiết bị tường lửa, đảm bảo tính an toàn bảo mật cao. Với mô hình này, tỉnh có thể trang bị firewall có cấu hình cao, chạy chế độ HA, đảm bảo tính sẵn sàng cao và đảm bảo cho lưu lượng vào các máy chủ không bị tắc nghẽn. Đồng thời, trang bị riêng database firewall đặt trước các máy chủ database, kiểm soát tất cả các hành động có tác động đến hệ thống cơ sở dữ liệu trong máy chủ, hỗ trợ tính năng bypass khi gặp sự cố, không ảnh hưởng đến hệ thống.

Hệ thống các máy chủ, lưu trữ có thể được tổ chức theo các lớp sau:



Ngoài ra, việc sử dụng tài nguyên các máy chủ vật lý hiệu quả cao mô hình điện toán đám mây ra đời dựa trên công nghệ ảo hóa đã giải quyết triệt để bài toán nâng cao hiệu suất phần cứng nhưng không phải mua sắm thêm thiết bị. Vì vậy, chúng tôi khuyến nghị lựa chọn mô hình điện toán đám mây là phù hợp nhất đối với TTDL của tỉnh Bình Phước. Để đảm bảo tính an ninh, an toàn với dữ liệu lưu hành nội bộ, mô hình điện toán đám mây (Private Cloud Computing) sẽ được áp dụng.

- **WAN Module**: Là thành phần hội tụ các kết nối mạng đến từ các đơn vị cấp Tỉnh, Huyện, Xã trên địa bàn tỉnh; ngoài ra còn có đường truyền kết nối giữa TTDL chính và TTDL dự phòng để đồng bộ và trao đổi dữ liệu giữa hai TTDL. Thành phần WAN bao gồm các WAN Router, WAN Firewall tích hợp IPS. Phân hệ WAN có thể trang bị thêm các thiết bị cân bằng tải để giảm tải cho DC tại lúc cao điểm hoặc khôi phục hệ thống từ DR. Cặp thiết bị này có thể hoạt động ở chế độ Active-Active hoặc Active-Standby;

- **Internet Module:** Là nơi tập trung toàn bộ các kết nối ra ngoài Internet, nơi này được bố trí thiết bị router để thực hiện các kết nối Internet. Module này có thể trang bị các thiết bị giảm thiểu DDoS , Internet Firewall tích hợp IPS, thiết bị cân bằng tải và tường lửa ứng dụng Web.

- **Partner Module**: Là nơi tập trung các kết nối cho các đơn vị bên ngoài có thể truy cập để

xử lý các yêu cầu trao đổi thông tin, liên thông quy trình, xử lý giao dịch (ví dụ: thanh toán điện tử…). Thành phần có thể gồm các Router, Firewall tích hợp IPS, thiết bị cân bằng tải.

- LAN Module: Là nơi cung cấp các cổng truy nhập vào mạng nội bộ cho người dùng tại TTDL. Thành phần của module này sẽ bao gồm các Distribution Switch và Access Switch. Chúng tôi khuyến nghị việc triển khai cácDistribution Switch và Access Switch cần đảm bảo phù hợp với số lượng người dùng thực tế và tính dự phòng, sẵn sàng cao. Riêng các Distribution Switch cần là các switch lớp 3, cung cấp chức năng định tuyến giữa các VLAN thông qua các giao thức định tuyến như RIP, EIGRP, OSPF. Việc triển khai HSRP (Hot-Standby Router Protocol) giữa các Distribution Switch cũng được khuyến nghị để đồng thời cho phép cân bằng tải và tăng cường khả năng sẵn sàng cao cho hoạt động ở lớp 3.

- Management Module: Thành phần cung cấp các dịch vụ quản trị mạng, quản trị an ninh, quản trị hệ thống server và storage, và hệ thống anti-virus. Thành phần bao gồm các phần mềm quản trị và thiết bị quản trị chuyên dụng. Các kết nối quản trị thông qua giao diện riêng độc lập với các kết nối truyền dữ liệu (OOB - Out of Band Management)

Ngoài ra, tại TTDL Chính, có thể đầu tư thêm Môi trường phát triển, kiểm thử, đào tạo, được xây dựng với mục đích tự lực phát triển, tổ chức thử nghiệm, tập huấn chuyển giao công nghệ cho các hệ thống trong tương lai cũng như kiểm tra, nâng cao trình độ các cán bộ kỹ thuật tỉnh Bình Phước, đảm bảo khả năng làm chủ các hệ thống CNTT trong tương lai.

c) Các giải pháp bảo mật cho TTDL

Quan điểm để xây dựng chính sách bảo mật: An ninh mạng là một tiến trình lặp đi lặp lại, bao gồm các bước xoay vòng như sau:

- Xác định các đối tượng cần được bảo vệ (máy chủ, các tài nguyên, các ứng dụng, các thiết bị mạng, máy trạm, người dùng…);

- Xác định các hiểm họa có thể gây nên cho mạng và hệ thống;

- Thiết lập chính sách an ninh cho mạng, bao gồm các nhà lãnh đạo, quản lý và tin học, quản trị mạng và người dùng;

- Thiết lập các chính sách an ninh mạng bằng các phương pháp điện tử và hành chính. Các phương pháp điện tử bao gồm: Thiết kế quy hoạch lại mạng, Firewall, VPN, IDS, ACS và quản trị an ninh mạng;

- Theo dõi an ninh mạng và phản ứng lại các biểu hiện bất thường;

- Kiểm tra chính sách an ninh và các thiết bị an ninh mạng để đáp ứng các thay đổi;

- Tiếp tục theo dõi và quản lý an ninh mạng, thay đổi chính sách an ninh và cấu hình các thiết bị an ninh mạng để phù hợp với ngữ cảnh an ninh mới.

Sau đây, chúng tôi đề xuất các giải pháp bảo mật cụ thể:

- Firewall

Là thiết bị tường lửa thế hệ mới. Với các tường lửa thế hệ mới này hệ thống có thể được bảo vệ từ lớp mạng đến lớp ứng dụng do Firewall thế hệ mới ngoài các tính năng quản lý truy cập dựa trên thông tin lớp mạng (IP) và lớp truyền dẫn (port), Firewall này còn có khả năng quản lý các

ứng dụng (hiểu được ứng dụng và can thiệp vào các tác vụ trong ứng dụng), người dùng. Firewall cũng cung cấp các tính năng quản lý băng thông để hệ thống mạng tối ưu hóa hiệu năng sử dụng. Ngoài ra trên Firewall thế hệ mới cũng có thêm các lựa chọn Anti-virus, Antispam, chống tấn công DoS… trong đó tính năng Anti-virus cũng có thể được dùng để cung cấp thêm một lựa chọn bảo vệ nữa cho hệ thống.

- **IPS (Intrusion prevention systems)**

Là thiết bị phát hiện và ngăn chặn tấn công. Thiết bị này giám sát luồng dữ liệu đi qua nó phát hiện những mẫu tấn công, các luồng dữ liệu bất thường, và dựa trên hành vi của các luồng dữ liệu mà chủ động ngăn chặn các tấn công. Thiết bị này có thể chống tấn công Malware, tấn công nhằm giảm hiệu năng thiết bị. Trong hệ thống có 2 lớp IPS, lớp thứ nhất để bảo vệ các Web Server và bảo vệ tấn công từ mạng bên ngoài, lớp thứ 2 bảo vệ các máy chủ ứng dụng và CSDL trong vùng Server Farm.

- **WAF**: Tường lửa ứng dụng web (Web Application Firewall - WAF)

Là một thiết bị phần cứng hoặc phần mềm được cài lên máy chủ có chức năng theo dõi các thông tin được truyền qua giao thức http/https giữa trình duyệt của người dùng và máy chủ web. Một WAF có khả năng thực thi các chính sách bảo mật dựa trên các dấu hiệu tấn công, các giao thức tiêu chuẩn và các lưu lượng truy cập ứng dụng web bất thường. Đây là điều mà các tường lửa mạng khác không làm được. Một số tính năng của thiết bị tường lửa ứng dụng Web (WAF):

- Cho phép nhận diện và xử lý các dạng tấn công phổ biến như XSS, CSRF, các loại tấn công Injection...
- Tự động xây dựng một mô hình bảo mật bảo vệ ứng dụng bằng cách liên tục theo dõi hoạt động của người dùng theo thời gian thực.
- Bảo vệ tấn công thay đổi giao diện web: Tự động phục hồi lại ứng dụng bằng các bản đã lưu khi phát hiện có tấn công thay đổi giao diện web.

- Giải pháp chống **DDoS** dựa trên DDoSAppliance: Ngày nay các cuộc tấn công từ chối dịch vụ DDoS là thách thức lớn nhất của các tổ chức cung cấp dịch vụ ra Internet như dịch vụ Cổng thông tin điện tử về dân cư. Các tiếp cận truyền thống như Firewall, IPS, WAF sử dụng cơ chế Stateful không ngăn chặn DDoS hiệu quả, nhiều khi còn chính là đối tường để các hacker thực hiện tấn công DDoS. Các tổ chức cần phải có một giải pháp hoàn toàn mới theo hướng Stateless. Giải pháp này thức hiện theo 4 bước:

1. Cài đặt DDoS Appliance ở vùng biên
2. Pháp hiện tấn công DDoS dựa trên stateless
3. Ngăn chặn
4. Cảnh báo

- **SIEM (Security information and event management):** Giải pháp hệ thống quản trị, phân tích log tập trung và quản lý sự kiện an ninh; thực hiện thu thập log từ nhiều nguồn khác nhau, phân tích và đánh giá mức độ an ninh và rủi ro của các sự kiện an toàn thông tin, nhanh chóng nhận diện, đánh giá mức độ và đáp trả các chính sách sai phạm, các tấn công từ bên ngoài và các mối đe dọa từ bên trong. Hỗ trợ xử lý sự cố: thông qua các công cụ phân tích điều tra, tạo luồng phối hợp

công việc xử lý sự cố, tạo lập cơ sở dữ liệu về các sự cố để tiện tra cứu sau này. Bên cạnh đó còn có các giải pháp quét virus trên các máy chủ, máy trạm và tại cổng kết nối với mạng bên ngoài mà điển hình là Internet. Ngoài ra là các giải pháp mạng riêng ảo (VPN) mã hóa các dữ liệu trên đường truyền, kiểm soát truy cập web (Web Filtering, URL Filtering) giảm thiểu các nguy cơ mất an toàn cho các máy trạm khi truy cập web, ngăn chặn thư rác (Spam Mail), ...

Mỗi sản phẩm bảo mật của mỗi nhà cung cấp có một thế mạnh riêng. Tuy nhiên mỗi hệ thống CNTT cần trang bị tối thiểu 3 giải pháp sau:

1. Giải pháp an ninh tích hợp: Tích hợp các tính năng như tường lửa (firewall), mạng riêng ảo (VPN), ngăn chặn xâm nhập (Intrusion Prevention - IPS), quét virus tại cổng kết nối mạng(anti-virus), kiểm soát truy cập web của các nhân viên (Web Filtering, URL Filtering)...;
2. Giải pháp phòng ngừa virus: Ngoài giải pháp an ninh tích hợp, cần vẫn thêm giải pháp phòng ngừa virus cho các máy chủ và các máy trạm.
3. Giải pháp quản trị phân tích log tập trung và quản lý sự kiện An ninh (SIEM)

Xu hướng của nhiều hãng bảo mật với các sản phẩm bảo mật đơn lẻ hiện nay là mở rộng, tích hợp thêm nhiều chức năng bảo mật khác thành một sản phẩm. Điển hình là nhiều sản phẩm firewall trước kia giờ đây được gọi là giải pháp tường lửa thế hệ mới (Next Generation Firewall - NGFW) với việc tích hợp các chức năng Firewall dựa trên công nghệ kiểm soát sâu vào gói tin (DPI - Deep Packet Inspection), IPS, URL filtering, Antivirus, Anti-spam, Anti-botnet,kiểm soát ứng dụng (Application Control), chống thất thoát dữ liệu (Data Loss Prevention)... trên cùng một thiết bị.

Ngoài ra, để đảm bảo an toàn của hệ thống đối với các lỗi logic trong dữ liệu của CSDL như tính toàn vẹn, hợp lý, đồng bộ dữ liệu, thay đổi cố ý về nội dung thông tin gây sai lệch đến tính đúng đắn của dữ liệu…, có thể áp dụng các giải pháp sau:

- Thiết lập tầng CSDL trung gian: Trong mô hình này, một CSDL trung gian (proxy) được xây dựng giữa ứng dụng và CSDL gốc. CSDL trung gian này có vai trò mã hóa dữ liệu trước khi cập nhật vào CSDL gốc, đồng thời giải mã dữ liệu trước khi cung cấp cho ứng dụng. CSDL trung gian đồng thời cung cấp thêm các chức năng quản lý khóa, xác thực người dùng và cấp phép truy cập;

- Sử dụng giải pháp tường lửa chuyên dụng cho cơ sở dữ liệu. Giải pháp chuyên dụng cần có các tính năng:

+ Quản lý rủi ro: Tìm và phân loại dữ liệu nhạy cảm bên trong CSDL, quét và phát hiện điểm yếu, cấu hình chưa tốt trên CSDL. Lập báo cáo phân tích rủi ro dựa theo quan hệ giữa điểm yếu và dữ liệu cũng như mức độ nhạy cảm của dữ liệu, trên cơ sở này lập chính sách bảo vệ và đưa ra biện pháp giảm nhẹ rủi ro.Với các điểm yếu được phát hiện, hệ thống cung cấp bản vá ảo (Virtual Patching) trên thiết bị cho phép bảo vệ các điểm yếu một cách nhanh chóng và trong suốt trong khi chưa thể thực hiện việc sửa chữa và cài đặt bản vá vào hệ thống CSDL;

+ Giám sát các truy cập tới dữ liệu nhạy cảm: Các giao dịch trên CSDL, đặc biệt các truy cập, tác động tới dữ liệu nhạy cảm được audit (ghi log) liên tục. Các thông tin Audit cung cấp đầy đủ chi tiết cho mỗi phiên giao dịch với CSDL như ai, thao tác lên đối tượng, dữ liệu nhạy cảm gì, sử

dụng công cụ, câu lệnh gì, thao tác như thế nào, khi nào và tại đâu,…Chức năng Audit hoạt động một cách độc lập với hệ quản trị CSDL, người quản trị CSDL không can thiệp được, không làm ảnh hưởng tới hiệu năng của máy chủ CSDL. Các thông tin Audit độc lập với CSDL và được lưu trữ bảo mật, cung cấp báo cáo, chứng cứ tin cậy khi xem xét các sự cố an ninh;

+ Kiểm soát truy cập CSDL: Giải pháp có thể nhìn sâu vào mọi hành động trên CSDL như các login, các truy vấn (SELECT), các thao tác của user cũng như của DBA (DML, DDL, DCL), các thay đổi liên quan đến dữ liệu, thủ tục, cấu trúc CSDL để giúp ngăn chặn các thao tác trái quyền.Chính sách bảo vệ dữ liệu được thiết lập để kiểm soát người dùng, ứng dụng và thao tác CSDL. Chính sách có thể quy định từ người dùng nào (user, DBA), sử dụng công cụ gì, được phép tác động tới đối tượng/dữ liệu gì, và được tác động dữ liệu như thế nào. Những thao tác trái quyền tới dữ liệu nhạy cảm có thể bị ngăn chặn hoặc cảnh báo vi phạm. Giải pháp có thể phân tích dữ liệu trả ra từ CSDL từ các câu lệnh truy vấn, kết quả trả ra chứa dữ liệu nhạy cảm có thể được cảnh báo hoặc ngăn chặn.Cơ chế tự học các giao dịch CSDL (Dynamic Profiling) cho phép hiểu các hoạt động bình thường, ngăn chặn các hành vi bất thường trái với quy luật thông thường. Dynamic Profiling sẽ học một (nhóm) người dùng, thường hay sử dụng công cụ gì, thường có những thao tác gì với những đối tượng dữ liệu nào và mức độ ra sao. Ví dụ việc truy vấn, hoặc sửa đổi số lượng bản ghi lớn vượt quá ngưỡng bình thường sẽ bị cảnh báo/ngăn chặn. Cung cấp chức năng IPS - phát hiện và ngăn chặn các tấn công trong thời gian thực tại mức hệ điều hành, mức giao thức cũng như mức các thao tác SQL, chống tấn công SQL Injection;

+ Quản lý thông tin phân quyền: Chức năng quản lý thông tin tài khoản - User Right Management (tùy chọn, cần mua thêm license), cho phép phân tích quyền được cấp cho tài khoản và đối tượng dữ liệu mà quyền tác động.

- Sử dụng cơ chế sẵn có trong CSDL:

+ Các hàm Stored Procedure trong CSDL cho chức năng mã hóa và giải mã;

+ Sử dụng cơ chế View trong CSDL tạo các bảng ảo, thay thế các bảng thật đã được mã hóa;

+ Cơ chế "instead of" trigger được sử dụng nhằm tự động hóa quá trình mã hóa từ View đến bảng gốc.

- Phân quyền truy cập dữ liệu theo vai trò của người dùng;

- Sử dụng cơ chế log của hệ quản trị CSDL để theo dõi, giám sát quá trình cập nhật dữ liệu;

- Thiết lập cơ chế backup định kỳ hoặc đột xuất dữ liệu cho hệ thống;

- Thiết lập các quy tắc cảnh báo trên hệ quản trị CSDL, cho phép thông báo tới quản trị hệ thống và ngăn chặn kịp thời các truy xuất bất thường đến hệ thống dữ liệu.

d) Hệ thống máy chủ

Hệ thống máy chủ và lưu trữ của Trung tâm dữ liệu được thiết kế để đáp ứng các tiêu chí quan trọng như sau:

Chức năng

- Tiêu chí đầu tiên và quan trọng khi thiết kế hệ thống là các khối chức năng trong hê thống trong TTDLS. Các chức năng chính của các cấu phần trong hệ thống bao gồm:

- Chức năng xử lý trong phân hệ ứng dụng được thiết kế cho các máy chủ ứng dụng Web/App

- Chức năng xử lý và quản trị Cơ sở dữ liệu tập trung, xây dựng trên các cặp máy chủ CSDL hoạt động ở chế độ song hành (clustering), cho phép xử lý và quản trị toàn bộ CSDL tập trung của Tỉnh.

- Chức năng quản trị thiết bị và hệ thống; được xây dựng phục vụ công tác quản trị thiết bị trong hệ thống, quản trị công tác sao lưu và khôi phục dữ liệu trong hệ thống

- Chức năng lưu trữ tập trung được phục vụ trên hệ thống lưu trư tập trung, với công nghệ hiện đại, đảm bảo tính sẵn sang và ổn định của toàn bộ dữ liệu của TTDL Tỉnh.

- Chức năng sao lưu và khôi phục dữ liệu: được quan tâm như là giải pháp đảm bảo sự an toàn của dữ liệu tập trung, trên cơ sở sử dụng những công nghệ sao lưu và khôi phục mới nhất, cùng phần mềm quản trị sao lưu tập trung.

Năng lực xử lý

- Tiêu chí năng lực xử lý của hệ thống được sử dụng nhằm xây dựng một hệ thống hạ tầng máy chủ, lưu trữ, sao lưu và khôi phục dữ liệu cho các hệ thống ứng dụng của Tỉnh, đáp ứng yêu cầu hiện tại và khả năng mở rộng trong tương lai.

- Tiêu chí năng lực xử lý được quan tâm đến khi lựa chọn công nghệ và thiết bị cho từng cấu phần trong hệ thống, cụ thể như sau:

- Hệ thống máy chủ CSDL sử dụng máy chủ có năng lức xử lý đáp ứng yêu cầu của ứng dụng nghiệp vụ và khả năng mở rộng trong tương lai

- Hệ thống máy chủ ứng dụng sử dụng máy chủ x86 có khả năng xử lý mạnh, với bộ xử lý Intel Xeon với tốc độ cao, nhiều nhân xử lý

- Hệ thống lưu trữ tập trung sử dụng thiết bị lưu trữ tầm trung, với tính sẵn sàng và độ ổn định cao nhất cho dữ liệu tập trung.

- Hệ thống SAN Switch sử dụng công nghệ xử lý và chuyển mạch tốc 10Gb FC, cho phép kết nối hệ thống máy chủ, hệ thống lưu trữ và sao lưu trong toàn bộ hệ thống với tốc độ cao.

Năng lực mở rộng

- Năng lực mở rộng của các thiết bị cũng là một tiêu chí được quan tâm khi thiết kế hệ thống. Các thiết bị chính được thiết kế cho phép mở rộng trong tương lai (trong nội bộ các thiết bị) và khả năng mở rộng về thiết kế.

- Khả năng mở rộng về thiết kế được thể hiện ở những điểm sau:

- Phân hệ ứng dụng (App Zone) được thiết kế cho phép mở rộng bằng các thêm các máy chủ vào Phân hệ ứng dụng

- Phân hệ CSDL được thiết kế với khả năng hoạt động song hành của cụm cluster với sự hỗ trợ xử lý song song

- Phân hệ lưu trữ được thiết kế với các SAN Switch kết nối dự phòng cao, khả năng mở rộng thông qua việc mở rộng cổng trên SAN Switch hoặc sử dụng công nghệ cascade các SAN

Switch với nhau.

Khả năng quản lý

- Tiêu chí về khả năng quản lý được đặt ra đảm bảo dễ dàng trong quá trình vận hành, khai thác hệ thống và khắc phục khi có sự cố xảy ra. Khả năng quản lý được xem xét khi lựa chọn các thiết bị trong hệ thống. Khả năng quản lý được đánh giá ở một số điểm sau:

- Khả năng quản lý thiết bị (Hardware)

- Khả năng quản lý môi trường (Hệ điều hành/cluster)

- Khả năng quản trị môi trường ảo hóa trên nền tảng VMWare

- Khả năng quản lý sao lưu và khôi phục dữ liệu

Tiết kiệm chi phí

- Tiêu chí tiết kiệm chi phí được xem xét khi lựa chọn thiết bị và giải pháp đảm bảo tiết kiệm trong đầu tư ban đầu, cũng như bảo vệ đầu tư trong tương lai.

Khả năng kết nối

- Thiết kế đáp ứng các yêu cầu chính đặt ra khi kết nối hệ thống các thiết bị trong hệ thống bao gồm:
- Đảm bảo kết nối giữa các thành phần hệ thống với nhau:
    - Các hệ thống máy chủ được kết nối với hạ thống mạng Ethernet, tốc độ 10Gb/s thông qua các cổng 10Gb trên các máy chủ
    - Các máy chủ ứng dụng Web/App đảm bảo kết nối với người dùng và kết nối với phân hệ dữ liệu (các máy chủ CSDL)
    - Các máy chủ CSDL kết nối với các máy chủ ứng dụng, các máy chủ quản trị sao lưu và khôi phục dữ liệu
    - Các hệ thống máy chủ cần kết nối với hệ thống lưu trữ được trang bị các HBA cung cấp các giao diện 10Gb Fibre Channel, để kết nối với mạng SAN tập trung
    - Các hệ thống lưu trữ tập trung, các hệ thống thư viện băng từ và máy chủ quản trị sao lưu và khôi phục dữ liệu được kết nối với nhau qua mạng SAN tốc độ cao, phục vụ công việc lưu trữ dữ liệu, sao lưu và khôi phục dữ liệu khi cần
- Đảm bảo băng thông:
    - Băng thông kết nối mạng Ethernet giữa các thiêt bị trong hệ thống được đảm bảo tốc độ 10Gb/s.
    - Băng thông kết nối các máy chủ với hệ thống SAN được thiết kế với tốc độ 8Gb/s thông quan mạng cáp quang SAN chuẩn FC. Hệ thống SAN switch với khả năng chuyển mạch cao sẽ đáp ứng yêu cầu hiện tại và mở rộng trong tương lai của hệ thống.
- Các hệ thống lưu trữ tập trung, hệ thống thư viện băng từ được kết nối với hệ thống SAN switch tốc độ cao, đảm bảo không tắc nghẽn khi phục vụ các ứng dụng.
- Đảm bảo tính sẵn sàng

- Mỗi máy chủ trong hệ thống: từ máy chủ ứng dụng, máy chủ CSDL đến các máy chủ quản trị, đều được trang bị ít nhất 2 card mạng tốc độ 10Gb/s, với 2 cổng trên 1 card, đảm bảo tính sẵn sàng cao nhất về kết nối từ các máy chủ đến hệ thống mạng Etnernet trung tâm
- Tương tự đối với các kết nối FC, các hệ thống máy chủ được trang bị HBA với 2 cổng FC, đảm bảo kết nối dự phòng đến hệ thống mạng SAN và đến các hệ thống lưu trữ và sao lưu tập trung.
- Hệ thống SAN switch được thiết kế dự phòng, bao gồm 02 SAN Switch, đảm bảo tính sẵn sàng cao từ các máy chủ đến hệ thống mạng SAN. Trong trường hợp 1 SAN Switch có sự cố, hệ thống vẫn hoạt động bình thường.

e) Hệ thống điều hành, giám sát an ninh mạng

Hệ thống điều hành, giám sát an ninh mạng phải đáp ứng các yêu cầu sau:

- Giám sát mạng:
    - Tình trạng hoạt động các thiết bị
    - Băng thông, đường truyền.
- Lập sơ đồ logic hoạt động toàn hệ thống
- Lập báo cáo chi tiết về hiệu năng toàn hệ thống
- Giám sát các ứng dụng như cơ sở dữ liệu, hệ thống email...
- Giám sát hệ thống ảo hóa
- Giám sát hệ điều hành
- Giám sát hệ thống Server
- Cảnh báo các yếu tố bất lợi đối với hệ thống qua hệ thống thư điện tử, SMS, RSS, WEB.

f) Hệ thống lưu trữ, sao lưu

Hệ thống lưu trữ đóng một vai trò hạt nhân vô cùng quan trọng trong một hệ thống. Với vai trò là thành phần trực tiếp lưu trữ dữ liệu tích hợp của tổ chức, thiết kế của hệ thống lưu trữ sẽ ảnh hưởng trực tiếp đến hiệu suất hoạt động, mức độ an toàn dữ liệu cũng như khả năng đáp ứng dịch vụ dữ liệu một cách liên tục của toàn bộ hệ thống. Giải pháp sao lưu, lưu trữ đảm bảo tuân thủ mô hình lưu trữ tập trung dựa trên công nghệ lưu trữ mạng tiên tiến nhất, đáp ứng các yêu cầu sau:

- Khả năng đáp ứng uyển chuyển (Scalability): Hệ thống phải có khả năng mở rộng dung lượng dễ dàng, nhanh chóng theo yêu cầu. Hệ thống lưu phải cho phép nâng cấp từ một volume (phục vụ một máy chủ) lên tới hàng nghìn volumes (phục vụ hàng nghìn máy chủ khác nhau) với chức năng nhiều truy cập đồng thời tới mỗi volume.

- Tính ổn định (Stability): Hệ thống lưu trữ phải được thiết kế để đảm bảo tối đa sự an toàn của dữ liệu, cũng như khả năng sẵn sàng phục vụ liên tục của dữ liệu. Hệ thống cũng cho phép triển khai các chức năng Disaster Recovery cho phép lưu trữ và phục hồi lại dữ liệu từ các thảm hoạ tồi tệ nhất (như cháy nổ, động đất ...)

- Tốc độ (Speed): Hệ thống lưu trữ phải có khả năng đáp ứng tốc độ kết nối cao, giảm thiểu thời gian truy cập cho người sử dụng và các ứng dụng.

- Khả năng chia sẻ, dùng chung dữ liệu (Shareability): Hệ thống cần được thiết kế cho phép hợp nhất dữ liệu trùng lặp, sao cho số lượng các bản sao vật lý của dữ liệu là tối thiểu, cùng với khả năng cho phép nhiều ứng dụng hay nhiều máy chủ với hệ điều hành khác nhau (Windows, Linux, Solaris, HP-UX, AIX…) có thể truy cập đồng thời vào các dữ liệu này.

- Tính đơn giản (Simplicity): Hệ thống lưu trữ phải được thiết để đơn giản hoá tối đa các thao tác quản trị, tích hợp và cấu hình cho phép triển khai hay nâng cấp nhanh chóng, sử dụng dễ dàng, nâng cao độ tin cậy và giảm các chi phí vận hành bảo trì sau này.

Hệ thống lưu trữ cung cấp khả năng quản lý lưu trữ tập trung, đảm bảo an toàn và cung cấp không gian lưu trữ cho các máy chủ trong toàn hệ thống như: máy chủ Database, máy chủ Mailbox Database và các máy chủ ảo hoá … có khả năng cung cấp mở rộng dung lượng lưu trữ khi cần thiết. Các yêu cầu đối với hệ thống lưu trữ tại TTDL:

- Tài nguyên phải được dự phòng với một mức độ nhất định để đảm bảo đáp ứng được các biến đổi bất thường về nhu cầu sử dụng tài nguyên tại một vài thời điểm nhất định.

- Các thiết bị máy chủ và lưu trữ phải đảm bảo dự phòng cho tất cả các thành phần và các kết nối. Nhằm giúp cho các ứng dụng có đủ tài nguyên để hoạt động một cách liên tục.

- Đảm bảo khả năng quản trị đơn giản, dễ dàng và tập trung. Đồng thời phải có khả năng backup và phục hồi nhanh nhất khi xảy ra sự cố.

Đối với hệ thống sao lưu thì hiện nay có hai loại công nghệ sao lưu đang được sử dụng phổ biến là:

- Công nghệ sao lưu ra băng từ (công nghệ truyền thống) hay còn được gọi là Disk to Disk to Tape.

- Công nghệ sao lưu ra tủ đĩa hay còn được gọi là Disk to Disk.

Công nghệ sao lưu băng từ gồm các giải pháp sau:

- Tape drive (thay băng tape bằng tay khi băng tape đầy dữ liệu):

+ DAT Drives: Là công nghệ tầm thấp thường dùng cho các doanh nghiệp nhỏ với độ tin cậy và chi phí thấp;

+ LTO (LTO1-200GB, LTO2-400GB, LTO3-800GB, LTO4-1.6TB, LTO5-3TB) Ultrium Drives: có dạng half- and full-height là loại cao cấp hơn DAT với băng tape dung lượng lớn hơn và hiệu suất cao hơn.

- **Tape Autoloader** được thiết kết theo kiểu nạp băng tape tự động (cho các băng tape trắng vào khe ổ tape sau đó băng nào đầy được tự động thay băng mới vào để backup tiếp dữ liệu) Tape Autoloader thường cho các công ty với các đặc điểm sau:

+ Ngăn chặn việc thay băng tape bằng tay mất thời gian và bị động, phải có người theo dõi khi băng tape đầy để thay băng mới;

+ Có dữ liệu nhiều hơn băng tape;

+ Hiệu suất cao, hiệu quả cao.

- **Tape Library:** Là thiết bị sao lưu dạng tự động, với dung lượng lớn (nguồn dữ liệu ở

nhiều nơi), thời gian nhanh, hiệu suất cao. Đây là giải pháp hoàn hảo, quản trị đơn giản, để dàng thao tác, vừa khít với nhiều môi trường của khách hàng, làm việc trên LAN, SAN, được trang bị những công cụ thông minh.

- **Phương thức sao lưu disk-to-disk** được phát triển để khắc phục thời gian truy nhập dữ liệu trong quá trình phục hồi. Sao lưu theo phương thức disk-to-disk (gọi ngắn gọn là d2d, hay còn được nhắc đến với thuật ngữ kỹ thuật disk-to-disk-to-tape hoặc tape-cache backup) về mặt vật lý là khi dữ liệu trước hết được sao lưu từ đĩa cứng sang đĩa cứng, thay vì sang băng từ như trong phương thức thông thường. Dữ liệu từ đĩa cứng sao lưu, sau khi được lưu trữ một thời gian dài cần thiết, mới được chuyển tiếp (sao chép, hoặc tạo bản clone) sang băng từ vật lý tại thời điểm được kích hoạt tùy theo nhu cầu của người quản trị. Như vậy quá trình phục hồi dữ liệu phần lớn sẽ là chuyển dữ liệu ngược lại từ đĩa cứng sang đĩa cứng, giảm thiểu được thời gian truy cập vào dữ liệu cần được phục hồi, và theo đó là giảm thời gian phục hồi dữ liệu.

2.5. Xác định các ứng dụng quản lý cơ sở hạ tầng và mô tả các yêu cầu cơ bản đối với các ứng dụng này

Các ứng dụng quản lý cơ sở hạ tầng là các dịch vụ mạng chia sẻ được sử dụng để quản lý hoặc tích hợp cơ sở hạ tầng khác.

- Quản lý cơ sở hạ tầng: Quản lý cơ sở hạ tầng là nền tảng phần mềm được sử dụng để thực hiện quản lý hệ thống, quản lý mạng và quản lý lưu trữ. Một số ví dụ về quản lý cơ sở hạ tầng. Dịch vụ này cho phép giám sát tổng thể toàn bộ các thành phần hạ tầng, đảm bảo nâng cao tầm nhìn hệ thống mạng, tìm ra những hỏng hóc trong hệ thống mạng, cải thiện tính sẵn sàng và hiệu năng của hệ thống mạng giữa các máy tính và các thiết bị nhằm đơn giản hóa việc trao đổi thông tin, chia sẻ nguồn lực và thông tin giữa các thiết bị được kết nối với nhau.

- Trao đổi thông tin và cộng tác: Trao đổi thông tin và cộng tác là các nền tảng phần mềm cho phép phân phối các kênh trực tuyến khác nhau, gồm trao đổi thông tin trên cơ sở thông điệp (message-based), thư điện tử (e-mail) và âm thanh (voice) hoặc hình ảnh (video). Một số ví dụ về Trao đổi thông tin và cộng tác. Các dịch vụ trao đổi thông tin và công tác bao gồm dịch vụ thư điện tử, lịch (calendar), địa chỉ liên lạc (contacts), và công việc (tasks); hỗ trợ truy cập thông tin trên thiết bị di động và trên nền web; hỗ trợ lưu trữ dữ liệu. Ngoài ra, còn có hệ thống quản lý cuộc gọi, đảm bảo có khả năng theo dõi tất cả các thành phần đang hoạt động trong hệ thống tổng đài điện thoại nội bộ truyền thống hoặc mạng VoIP; những thành phần này gồm có điện thoại, cổng nối (gateway), cầu hội nghị (conference bridges), nguồn chuyển mã (transcoding resources), và hộp thư thoại (voicemail)...

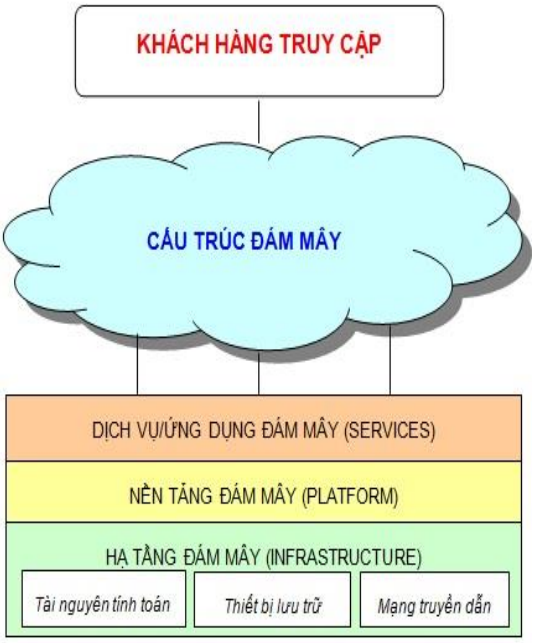
- Các dịch vụ thư mục: Dịch vụ thư mục là hệ thống phần mềm lưu trữ, tổ chức và truy cập thông tin trong một thư mục. Trong kỹ thuật phần mềm, một thư mục là một sơ đồ giữa các tên và các giá trị. Nó cho phép tra cứu các giá trị được gán vào một tên, tương tự như một cuốn từ điển. Giống như một từ trong từ điển có thể có nhiều định nghĩa, trong một thư mục một tên cũng có thể liên quan đến nhiều mảng thông tin khác nhau. Tương tự như vậy, một từ có thể có các dạng từ loại khác nhau và các định nghĩa khác nhau, do đó, một tên trong thư mục cũng có thể có nhiều loại dữ liệu khác nhau.

- Quản lý cấu hình: Quản lý cấu hình là các nền tảng phần mềm cho phép kiểm soát tập trung dựa trên các cơ sở hạ tầng khác nhau sẵn có trên mạng như quản lý các máy tính/nhóm máy tính lớn trong hệ thống cũng như cung cấp chức năng quản lý từ xa, vá lỗi, phân phối phần mềm, triển khai hệ điều hành, bảo vệ truy cập hệ thống mạng, và kho lưu trữ phần cứng, phần mềm.

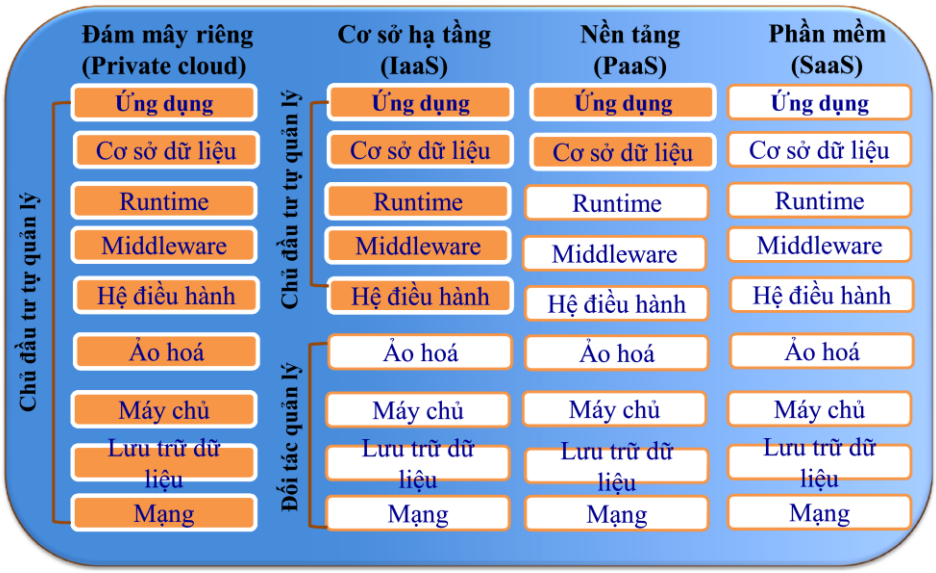
- Quản lý đám mây riêng" Quản lý đám mây riêng là một bộ nền tảng phần mềm mở rộng nền tảng ảo hóa cơ bản cho phép cung cấp mô hình điện toán đám mây "cơ sở hạ tầng như một dịch vụ" trong tỉnh. Giải pháp quản lý đám mây riêng cần có khả năng trừu tượng hóa các nguồn lực ảo hóa để cho phép người dùng tự truy cập vào các nguồn lực này thông qua một danh mục dịch vụ.

2.6. Điện toán đám mây trong phát triển Chính quyền điện tử tỉnh Bình Phước

Ngoài việc áp dụng các chuẩn, kiến trúc trong Chính quyền điện tử, để triển khai Chính quyền điện tử thành công đòi hỏi phải tận dụng được sức mạnh của công nghệ mới, công nghệ mới sẽ giúp quá trình triển khai nhanh hơn, hiệu quả kinh tế cao hơn. Một trong những công nghệ nổi bật, là xu thế ứng dụng CNTT trong trong xã hội nói chung và Chính quyền điện tử nói riêng đó là "Điện toán đám mây" (Cloud computing). Điện toán đám mây cho phép thực hiện việc ảo hóa các tài nguyên tính toán và các ứng dụng. Thay vì việc sử dụng một hoặc nhiều máy chủ (server) thật, thì nay sử dụng các tài nguyên được ảo hóa (virtualized) thông qua môi trường Internet. Mô hình điện toán đám mây được minh họa như hình sau.



Dịch vụ Điện toán đám mây (ĐTĐM) rất đa dạng và bao gồm tất cả các lớp dịch vụ điện toán từ cung cấp năng lực tính toán trên mạng lưới máy chủ hiệu năng cao hay các máy chủ ảo, không gian lưu trữ dữ liệu, hay một hệ điều hành, một công cụ lập trình, một ứng dụng kế toán,... Các dịch vụ cũng được phân loại khá đa dạng, nhưng các mô hình dịch vụ ĐTĐM phổ biến nhất có thể được phân thành ba nhóm: Dịch vụ hạ tầng (**IaaS**-Infrastructure as a Service), Dịch vụ nền tảng (**PaaS**- Platform as a Service) và Dịch vụ phần mềm (**SaaS**- Software as a Service). Sau đây là các mô tả khái quát về các mô hình dịch vụ này:



Đám mây công cộng (Public Cloud)

Các đám mây công cộng là các dịch vụ đám mây được một bên thứ ba (người bán) cung cấp. Chúng tồn tại ngoài tường lửa cơ quan và chúng được nhà cung cấp đám mây quản lý. Cho dù đó là phần mềm, cơ sở hạ tầng ứng dụng hoặc cơ sở hạ tầng vật lý, nhà cung cấp đám mây chịu trách nhiệm về cài đặt, quản lý, cung cấp và bảo trì. Khách hàng chỉ chịu phí cho các tài nguyên nào mà họ sử dụng.

Đám mây riêng (Private Cloud)

Các đám mây riêng là các dịch vụ đám mây được cung cấp trong tổ chức nên còn có tên gọi là đám mây "cơ quan". Những đám mây này tồn tại bên trong tường lửa cơ quan và chúng được cơ quan quản lý. Các đám mây riêng đưa ra nhiều lợi ích giống như các đám mây công cộng thực hiện với sự khác biệt chính: cơ quan có trách nhiệm thiết lập và bảo trì đám mây này. Việc kiểm soát chi tiết hơn trên các tài nguyên khác nhau đang tạo thành một đám mây mang lại cho cơ quan tất cả các tùy chọn cấu hình có sẵn. Ngoài ra, các đám mây riêng là lý tưởng cho các kiểu công việc đang được thực hiện không phù hợp cho một đám mây chung, ví dụ như về an ninh, quản lý.

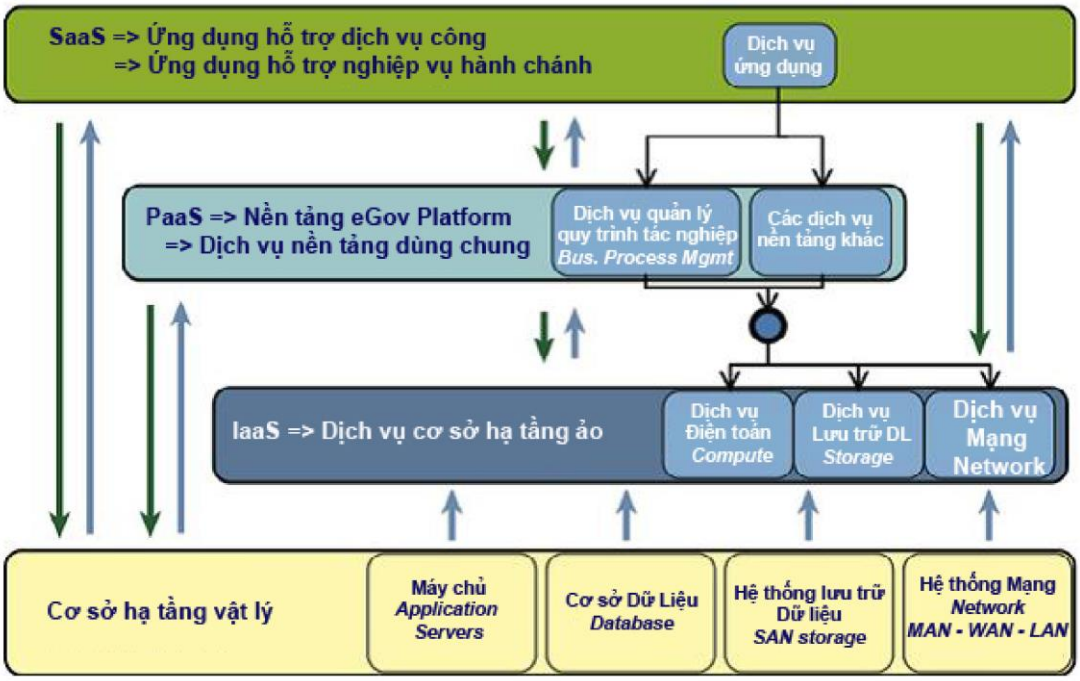
Đám mây "cộng đồng" (Community Cloud)

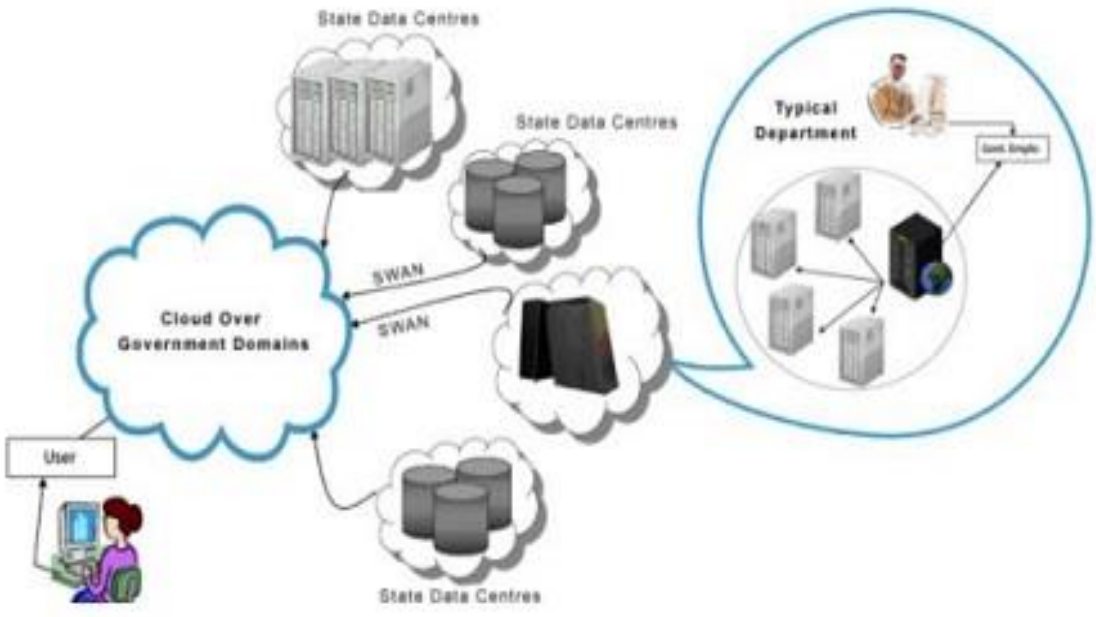
Đám mây "cộng đồng" là mô hình trong đó hạ tầng đám mây được sử dụng và quản lý bởi một số tổ chức cộng đồng người dùng. Các tổ chức này có đặc thù không tiếp cận với các dịch vụ Public Cloud và chia sẻ chung một hạ tầng ĐTĐM để nâng cao hiệu quả đầu tư và sử dụng.

Đám mây lai (Hybrid Cloud)

Mô hình đám mây lai là sự kết hợp đám mây công cộng và riêng. Trong mô hình này thông thường những thông tin có thể công khai trên diện rộng được đặt trên đám mây công cộng, còn những thông tin nghiệp vụ cần bảo mật cao hơn được đặt trên đám mây riêng.

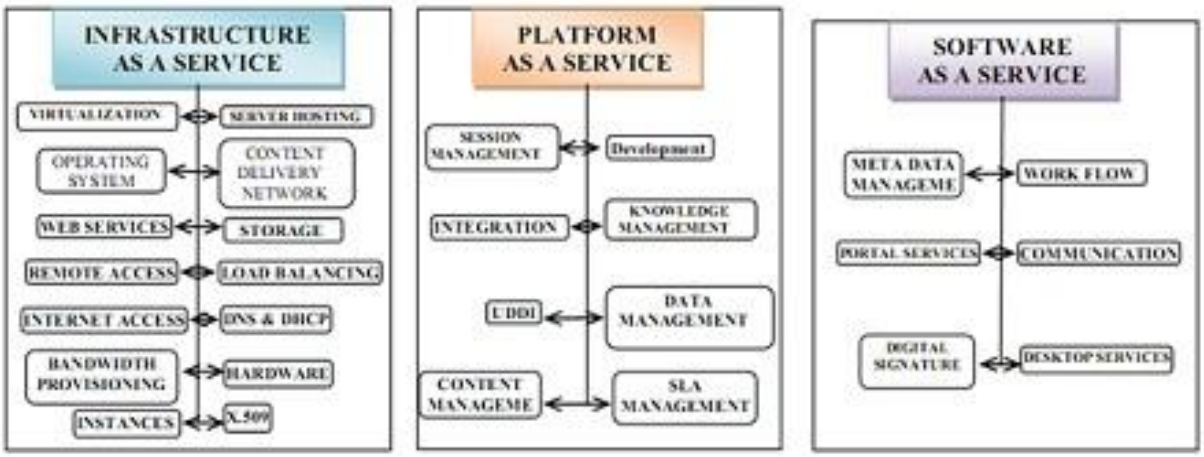
Sau đây chúng tôi đề xuất mô hình áp dụng điện toán đám mây cung cấp dịch vụ công trực tuyến (G-cloud).





Qua mô hình trên ta thấy các Hệ thống thông tin/trung tâm dữ liệu của các cơ quan nhà nước được kết nối với nhau qua mạng diện rộng của Chính phủ, tạo ra đám mây. Người sử dụng có thể truy cập các dịch vụ thông qua đám mây của Chính phủ này.

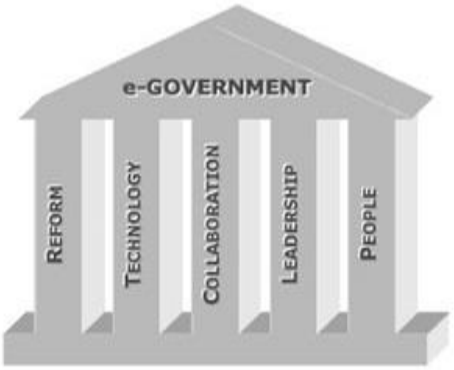
Tại các lớp dịch vụ, cơ quan chính phủ có thể triển khai các ứng dụng khác nhau, hình sau minh họa các thành phần tại các lớp của đám mây cung cấp dịch vụ công trực tuyến.



Qua hình trên ta thấy cơ quan chính phủ có thể thuê dịch vụ hạ tầng (IaaS) như: phần ứng tính toán, lưu trữ, hệ điều hành, mạng, truy cập từ xa, máy chủ,...; dịch vụ nền tảng (PaaS) như: quản trị nội dung, tri thức, tích hợp, quản lý giao dịch, dữ liệu,...; dịch vụ phần mềm (SaaS) như: quản lý đặc tả dữ liệu (metadata), dịch vụ cổng (portal), quản lý luồng công việc, chữ ký số, các dịch vụ, phần mềm chạy trên các máy tính cá nhân,... Với khả năng ứng dụng đa dạng, mềm dẻo như trên, qua khảo sát cho thấy đa số mọi người đều quan tâm phát triển ĐTĐM trong Chính quyền điện tử, đồng thời có quan điểm về những chức năng của ĐTĐM khi ứng dụng.

Để có thể ứng dụng ĐTĐM trong Chính quyền điện tử, cần xác định được những yếu tố thành công, những lợi ích của điện toán đám mây có thể mang lại, đồng thời phải xác định được rủi ro có thể xảy ra để lường trước.

Những nhân tố thành công



Leadership- Lãnh đạo

Vai trò lãnh đạo chính trị mạnh mẽ của Chính phủ là yếu tố quan trọng trong việc thiết lập cơ chế phối hợp chặt chẽ giữa các bộ, ngành khi phát triển Chính quyền điện tử. Yếu tố này liên quan đến việc đưa ra các quy định về việc phân bổ đủ nguồn lực, phân quyền, báo cáo đôn đốc triển khai. Áp dụng công nghệ mới trong các quy trình cốt lõi của các cơ quan chính phủ giao tiếp với khách hàng (người dân, doanh nghiệp) đòi hỏi một sự lãnh đạo khôn ngoan, bảo đảm sự cân bằng hợp lý giữa lợi ích tiềm năng và các rủi ro có thể gặp phải. Sự lãnh đạo mạnh mẽ là cần thiết ngay từ pha thiết kế các hệ thống Chính quyền điện tử, bảo đảm giải quyết các xung đột, tính kết

nối, liên thông giữa các hệ thống khi áp dụng ĐTĐM.

Reform - Cải cách

Nhiều nước đang phát triển vẫn có nền hành chính chủ yếu dựa trên giấy tờ theo mô hình truyền thống. Việc thay đổi những quy trình nghiệp vụ hiện hành nhằm phân định rõ chức năng của các đơn vị hành chính, tạo sự kết nối, chia sẻ thông tin trong phát triển Chính quyền điện tử là rất khó khăn, đòi hỏi phải có sự chỉ đạo, triển khai quyết liệt của các cấp. Mặt khác, ĐTĐM trong khu vực công có thể dẫn đến những kết quả không mong muốn hoặc ảnh hưởng phụ khó kiểm soát hơn. Chính vì vậy, mục tiêu đính của việc cải cách là cho phép cung cấp các dịch vụ đặc thù hơn, chuyên nghiệp hơn hướng tới nền hành chính hiện đại, hiệu quả hơn.

People - Con người

Yếu tố con người luôn là trung tâm trong mọi thành công. Để có sự đồng thuận, góp sức của con người phát triển Chính quyền điện tử, trong quá trình triển khai cần chú ý đến những phản hồi từ phía người dùng, để bảo đảm đáp ứng mức độ hài lòng cao nhất. Cụ thể, khi triển khai các hệ thông thông tin trong Chính quyền điện tử, áp dụng ĐTĐM cần phải phát triển các tùy biến mềm dẻo phù hợp với cơ quan chính quyền địa phương và các cơ quan chuyên ngành.

Technology- Công nghệ

Các cơ quan chính phủ tạo ra một số lượng lớn các dữ liệu có cấu trúc hoặc phi cấu trúc, các dữ liệu này cần được phân tích, xử lý, kết nối. Quá trình lưu trữ, truy cập, và xử lý khối dữ liệu lớn như vậy cần được coi như là một thách thức lớn, cơ bản để triển khai các dịch vụ Chính quyền điện tử. ĐTĐM hy vọng cung cấp một nguồn tài nguyên tính toán không hạn chế, với khả năng truy cập bất cứ đâu.

Collaboration- Hợp tác

Các dịch vụ Chính quyền điện tử cần được cung cấp tới người dân và doanh nghiệp nhanh chóng, đồng thời có thể phục vụ nhiều đối tượng trên phạm vi địa lý khác nhau. Thêm vào đó, những người sử dụng có thể chạy các ứng dụng giống nhau trên các cơ sở dữ liệu khác nhau. Do vậy, hợp tác là vấn đề quan trọng, cốt yếu để ứng dụng công nghệ ĐTĐM, tránh việc triển khai trùng lặp. Trong thực tế, nhiều cơ quan chính phủ có nhu cầu xử lý thông tin giống nhau hoặc tương tự nhau, như vậy các yêu cầu chức năng đối với phần mềm cũng tương tự nhau. ĐTĐM có thể được coi là một trong các giải pháp tốt nhất trong những trường hợp này, cho phép cung cấp phần mềm như là một dịch vụ, các cơ quan chính phủ sử dụng cùng một phần mềm với sự thay đổi nhỏ tùy theo nhu cầu từng cơ quan. Sự thay đổi này trong ĐTĐM chỉ ảnh hưởng đến đặc tả dữ liệu (metadata), mà không ảnh hưởng đến mã nguồn của ứng dụng.

Những lợi ích tiềm năng

Rapid Elasticity - Tính mềm dẻo, đáp ứng nhanh

Điện toán đám mây được thiết kế để cung cấp các dịch vụ với khả năng mở rộng không giới hạn, đây được coi là một trong các đặc điểm cơ bản của nó. Khách hàng có thể truy cập một kho tài nguyên rộng lớn được ảo hóa, cho phép đáp ứng các nhu cầu tài nguyên không định trước một cách hiệu quả và kinh tế. Khách hàng chỉ phải trả phí cho những tài nguyên thực dùng, được kiểm soát tự động theo thời gian thực. Bởi vậy, hiệu năng và tính bền vững kinh tế của hệ thống

được cân đối hài hòa.

Maintenance and Technical Support - Hỗ trợ kỹ thuật và duy trì

Những nhà cung cấp dịch vụ điện toán đám mây quản lý, duy trì các ứng dụng, máy chủ, họ cũng thực hiện công tác nâng cấp phần mềm, triển khai các hỗ trợ kỹ thuật chuyên nghiệp. Việc duy trì, cài đặt, nâng cấp phần mềm sẽ được thực hiện trên đám mây mà không cần thực hiện trên máy tính của khách hàng. Đây thực sự là một lợi điểm nổi bật của ĐTĐM, đặc biệt đối với các cơ quan chính phủ ở các nước đang phát triển, hoặc ở khu vực nông thôn khi mà khó có thể thu hút đủ nhân lực công nghệ thông tin để duy trì, cập nhật hoạt động của các hệ thống thông tin.

Cost Effectiveness - Hiệu quả chi phí

Các mô hình dịch vụ điện toán đám mây hiện nay đều tập trung cung cấp các dịch vụ hiệu quả về chi phí. Chúng tạo ra một cơ hội để dịch chuyển từ chi phí đầu tư sang chi phí vận hành, tránh được việc phải đầu tư lớn để mua các hệ thống thông tin đắt tiền, thuê đội ngũ cán bộ kỹ thuật trình độ cao để quản lý, duy trì hệ thống Chính quyền điện tử.

Disaster Recovery - Khắc phục thảm họa

Một trong các yêu cầu tối quan trọng đối với hạ tầng công nghệ thông tin là khả năng chịu đựng trước các thảm họa. Đối với ĐTĐM, nhà cung cấp dịch vụ thường đưa ra nhiều phương án lựa chọn hơn so với mô hình truyền thống để khôi phục dữ liệu nhanh chóng, hiệu quả khi có thảm họa. Bằng việc sử dụng đám mây như là môi trường sao lưu dự phòng, các cơ quan chính phủ sẽ tiết kiệm chi tiêu đầu tư hệ thống dự phòng, đồng thời tính an toàn cao hơn khi dữ liệu được sao lưu tại nhiều địa điểm dự phòng trên đám mây.

Green ICT Eco-Friendly Systems- Các hệ thống công nghệ thông tin - truyền thông xanh thân thiện môi trường

Việc tăng lên theo hàm mũ số lượng thiết bị công nghệ thông tin và truyền thông trong các cơ quan chính phủ đã gây ảnh hưởng xấu đến môi trường, làm tăng phát xạ đi-ô-xít các bon do tiêu thụ năng lượng nhiều hơn. ĐTĐM là công nghệ thích hợp làm giảm tiêu thụ năng lượng và cung cấp các hệ thống thân thiện môi trường thông qua các dịch vụ được ảo hóa. Sử dụng các dịch vụ ảo hóa có thể sẽ giảm đến 90% nguồn năng tiêu thụ của các máy tính cá nhân tiêu biểu.

Các rủi ro

Để ứng dụng công nghệ ĐTĐM trong Chính quyền điện tử, ngoài hiểu biết các ưu điểm, lợi thế của công nghệ này, chúng ta cần có những hiểu biết về những mối đe dọa, rủi ro để phòng tránh. Phần sau đây sẽ mô tả những rủi ro chính cần được quan tâm.

Các rủi ro an ninh (Security risks)

An ninh của hệ thống (security) được hiểu là khả năng của hệ thống ngăn ngừa, chịu đựng trước những tấn công gây tổn hại. Có bảy rủi ro an ninh chính liên quan đến mô hình ứng dụng ĐTĐM. Bao gồm:

- Truy cập (Access): Do dữ liệu phân tán tại các vị trí địa lý khác nhau, trên các thiết bị vật lý khác nhau, có nhiều đối tương truy cập, nên nếu những dữ liệu nhạy cảm không duy trì được cơ chế phân lập, bảo vệ hợp lý, thì sự xâm phạm các dữ liệu này có nguy cơ cao. Mặt khác, các cơ

quan chính phủ cũng phải ban hành các chính sách, thể chế rõ ràng về truy cập thông tin Chính phủ.

- Tính sẵn sàng (Availability): Tính sẵn sàng dịch vụ trong ĐTĐM đóng vai trò rất quan trọng đối với khách hàng. Một nghiên cứu của Trường đại học California về tính sẵn sàng và sự gián đoạn cung cấp dịch vụ của 4 nhà cung cấp dịch vụ điện toán đám mây lớn chỉ ra rằng các quá tải hệ thống đã gây ra các lỗi chương trình, điều này gây lỗi, gián đoạn dịch vụ. Mặt khác, các thảm họa thiên nhiên cũng là rủi ro tiềm tàng làm gián đoạn các dịch vụ ĐTĐM. Đã có hiện tượng sét đánh các thiết bị ĐTĐM và làm gián đoạn dịch vụ. Tính sẵn sàng ở đây cần được hiểu thêm nghĩa là quá trình cung cấp dịch vụ liên tục trong thời gian dài, các dịch vụ ĐTĐM được thuê từ nhà cung cấp, vậy cần lường trước khả năng họ ngừng cung cấp dịch vụ do một lí do bất khả kháng nào đó, ví dụ chuyển mục tiêu kinh doanh, thậm trí phá sản.

- Tải mạng (Network load): Tải mạng đám mây cũng là vấn đề cần quan tâm. Nếu dung lượng sử dụng tài nguyên mạng trên 80% thì các máy tính có thể trở thành không đáp ứng, hoặc giảm hiệu năng tính toán (do nhà cung cấp có cơ chế bảo vệ thiết bị của họ), đặc biệt khi xử lý, trao đổi dữ liệu lớn.

- Tính toàn vẹn (Integrity): Tính toàn vẹn dữ liệu ảnh hưởng đến độ chính xác của thông tin trong hệ thống. Trong môi trường ĐTĐM, tính hiệu lực, chất lượng, mức độ an toàn, an ninh của dữ liệu ảnh hưởng đến hoạt động của hệ thống và kết quả đầu ra. Nhà cung cấp dịch vụ ĐTĐM phải có cơ chế bảo đảm tính toàn vẹn của dữ liệu trong các tình huống xảy ra. Ví dụ như mất dữ liệu, đám mây không sẵn sàng.

- An ninh dữ liệu (Data Security): Cần bảo đảm dữ liệu phải được bảo vệ, với ĐTĐM, số tổn hại dữ liệu tăng lên khi dữ liệu được chia sẻ tùy tiện trong nhiều hệ thống khác nhau trên đám mây, đặc biệt là các hệ thống thông tin của Chính quyền điện tử. Đây là điều mà các nhà cung cấp dịch vụ hết sức lưu ý để có các cơ chế phù hợp.

- Vị trí dữ liệu (Data location): Trong ĐTĐM, về nguyên tắc, dữ liệu được phân tán trên toàn cầu, điều này tạo nên sự nhận biết không rõ ràng của khách hàng về vị trí chính xác dữ liệu của họ trên đám mây, gây khó khăn cho việc quản lý, điều tra nếu có vấn đề.

- Sự phân lập dữ liệu (Data Segregation): Sự phân lập dữ liệu là điều khó khăn trên tất cả môi trường ĐTĐM, do tất cả các dữ liệu không thể được biệt lập theo nhu cầu của người sử dụng. Đây cũng là yếu tố rủi ro cần lường trước trên môi trường ĐTĐM trước những truy nhập trái phép dữ liệu.

Các rủi ro về tính riêng tư (Privacy risks)

Có một vài vấn đề về tính bảo mật và riêng tư phức tạp liên quan đến ĐTĐM. Thực ra, chưa có quy định hạn chế người dùng phơi bày các thông tin cá nhân trên đám mây. Việc này đôi khi dẫn đến những hậu quả nghiêm trọng. Vấn đề càng trở lên phức tạp nếu thông tin được đưa lên các đám mây xuyên biên giới, khi đó những quy định về bảo mật tính riêng tư ở các nước khác nhau là khác nhau, rất khó xử lý những sự cố xảy ra.

Các rủi ro người tiêu dùng (Consumer risks)

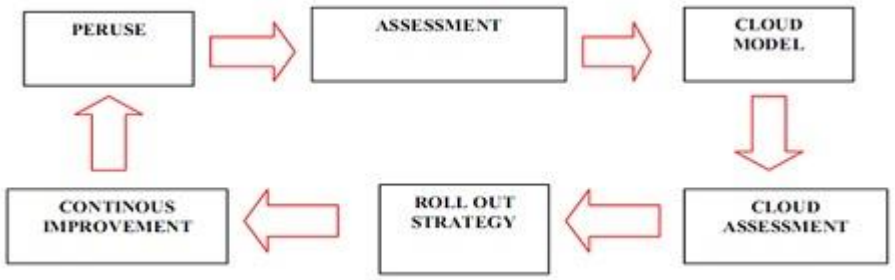
Việc sử dụng ĐTĐM có thể gây một số rủi ro cho người tiêu dùng, đối với Chính quyền

điện tử chính là các cơ quan chính phủ. Việc cung cấp dịch vụ phụ thuộc vào hợp đồng được dự thảo sẵn bởi nhà cung cấp, thường không có đóng góp gì từ phía khách hàng. Đôi khi nhà cung cấp thay đổi một số điều khoản liên quan đến việc cung cấp sản phẩm mà khách hàng không nhận biết được vấn đề này. Những sự thay đổi đột ngột, không thông báo có thể dẫn tới các rủi ro cho người tiêu dùng. Để phòng tránh các rủi ro người tiêu dùng và rủi ro về tính riêng tư, người tiêu dùng cần làm quen với sản phẩm ĐTĐM, và điều kiện của nó trước khi dùng. Ví dụ khi sử dụng sản phẩm Docs của Google, cần đọc tối thiểu các thông tin sau: các điều khoản dịch vụ chung, các điều khoản phụ thêm, các chính sách chương trình, chính sách riêng tư, các lưu ý về bản quyền.

Lộ trình triển khai ứng dụng công nghệ điện toán đám mây

Để chuyển sang ứng dụng ĐTĐM trong Chính quyền điện tử, cần phải có bước đi, lộ trình hợp lý và phải phù hợp vào điều kiện, nhu cầu thực tế trên cơ sở phân tích những ưu thế khi sử dụng ĐTĐM, nhưng cũng phải lường trước những khó khăn, rủi ro có thể xảy ra.

Từ kinh nghiệm triển khai, một số học giả trên thế giới đã đề xuất một số bước đi, lộ trình cụ thể triển khai ĐTĐM. Sau đây là đưa ra mô hình sáu bước chuyển sang ứng dụngĐTĐM:



(1) Xem xét kỹ - *Peruse*:

Bước đầu tiên là cần phải nghiên cứu, học tập những kiến thức cơ bản nhất của ĐTĐM. Cần nâng cao nhận thức, đào tạo nhân lực liên quan đến phát triển Chính quyền điện tử về công nghệ ĐTĐM. Cần đầu tư kinh phí nghiên cứu khả năng ứng dụng ĐTĐM, xây dựng chính sách áp dụng.

(2) Đánh giá - *Assessment*:

Trong bước thứ hai, các nhân viên CNTT hoặc nhân viên chính phủ đưa ra đánh giá những nhu cầu, cấu trúc, năng lực ứng dụng CNTT hiện hành. Ví dụ nhu cầu tăng hay giảm tài nguyên thông tin.

(3) Mô hình đám mây - *Cloud Model*:

Trong bước thứ ba, các chuyên gia CNTT sẽ phát triển một mô hình mẫu ứng dụng ĐTĐM dựa trên những yêu cầu bằng việc thực hiện một dự án cụ thể.

(4) Đánh giá đám mây - *Cloud Assessment*:

Sau khi có những đánh giá bên trong, bên ngoài đối với mô hình mẫu thử nghiệm, các chuyên gia CNTT nên có đánh giá chung về khả năng ứng dụng ĐTĐM tại cơ quan, và mô hình nào (đám mây công cộng/riêng/lai...) là phù hợp cho cơ quan. Những ứng dụng, dữ liệu gì có thể chuyển lên đám mây.

(5) Triển khai chiến lược - *Roll out strategy*:

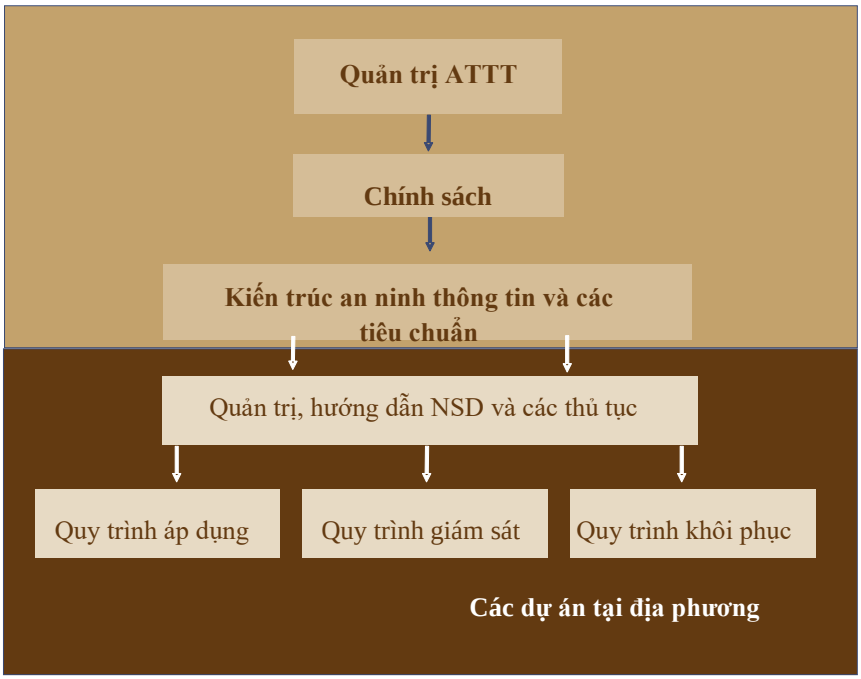
Trong bước này, bắt đầu triển khai chiến lược ứng dụng công nghệ ĐTĐM trên diện rộng bằng cách triển khai các dự án áp dụng ĐTĐM, cần quan tâm nhiều vấn đề như lãnh đạo, cán bộ CNTT, truyền thông bên trong và bên ngoài.

(6) Tiếp tục cải thiện - *Continous improvement*:

Bước này được tiến hành để bảo đảm hệ thống đám mây có đầy đủ chức năng mong muốn.

2.7. Xác định mô hình triển khai đảm bảo ATTT tổng thể của tỉnh; xác định các thành phần then chốt và mô tả yêu cầu căn bản đối với các thành phần

Ngày nay, những rủi ro về thông tin cũng đã tăng lên gấp nhiều lần do việc ứng dụng những công nghệ mới. An toàn không chỉ là việc giữ bí mật dữ liệu mà còn phải bảo vệ tính toàn vẹn, cách thức truy nhập và tính sẵn có của dữ liệu. An toàn là cần thiết để thiết lập và giữ vững uy tín giữa các cơ quan chính quyền và người dân, những người đang sinh sống tại địa phương và các doanh nghiệp. Thông tin kịp thời và tin cậy là cần thiết để xử lý giao dịch và hỗ trợ hoạt động của từng cơ quan. Với các dự án CPĐT thì mức độ phụ thuộc vào thông tin lại càng cao, và bất kì sự rò rỉ thông tin hoặc không bảo đảm tính toàn vẹn của thông tin cũng sẽ ảnh hưởng trực tiếp đến lợi ích của tỉnh Bình Phước.



Mô hình kiến trúc bảo mật

Mức độ rủi ro về an toàn thông tin đang tiếp tục tăng lên và cao hơn bao giờ hết. Để giải quyết được vấn đề này không chỉ cần có công cụ kiểm soát an toàn là đủ. Bảo vệ an toàn là một quá trình liên tục, trong đó các công cụ kiểm soát chỉ là một yếu tố của cả hệ thống. Các yếu tố khác bao gồm năng lực của nhân viên CNTT trong việc thường xuyên tự đánh giá khả năng của mình và đối phó kịp thời với các nguy cơ mới trong môi trường công nghệ và nghiệp vụ thường xuyên thay đổi. Để thiết lập và duy trì hệ thống an toàn thông tin một cách hiệu quả thì chính quyền tỉnh Bình Phước cần phải thống nhất các quy trình, con người và công nghệ để giảm bớt rủi ro, phù hợp với chính sách quản lý rủi ro và giữ mức độ rủi ro ở giới hạn cho phép. Điều này có thể được

thực hiện bằng cách xây dựng một quy trình xác định rủi ro và đưa ra chiến lược phù hợp để thực thi. Chiến lược này cần được thử nghiệm một cách có cấu trúc và được giám sát thường xuyên. Để bảo đảm tính hiệu quả của hệ thống an toàn thông tin của tỉnh Bình Phước, cần có khung an toàn thông tin đa cấp. Hình trên đây đề xuất kiến trúc an toàn thông tin cho các sở, ban, ngành ở tỉnh Bình Phước và đề xuất này cũng là một phần của CPĐT.

2.7.1 Chính sách quản trị an toàn trung tâm

Tất cả các ứng dụng và cơ sở hạ tầng được sử dụng và quản lý trong các dự án CPĐT là các hệ thống có tầm quan trọng quốc gia và đòi hỏi phải có hệ thống an toàn đầy đủ. Để bảo đảm hệ thống an toàn được xây dựng một cách nhất quán và đầy đủ, cán bộ lãnh đạo CNTT cần tập trung thực hiện một số công việc sau:

- Thành lập một hội đồng quản trị an toàn.

- Xây dựng chính sách an toàn cho tỉnh Bình Phước

- Xây dựng các kiến trúc và tiêu chuẩn an toàn.

Những công việc dù được thực hiện ở cấp Tỉnh vẫn cần phải được áp dụng cho tất cả các cơ quan, đơn vị.

Hội đồng quản trị an toàn

Nhằm quản lý hiệu quả hệ thống an toàn cho các đơn vị trên toàn tỉnh, cần thành lập một hội đồng quản trị an toàn tập trung. Ngoài việc giám sát và nâng cấp các chương trình bảo mật, hội đồng này có trách nhiệm xây dựng và phê duyệt các chính sách bảo vệ an toàn. Trách nhiệm của hội đồng quản trị an toàn là:

- Xác định và điều hành các mục đích, chiến lược, chính sách và nâng cao nhận thức về an toàn thông tin trong toàn Tỉnh.

- Phê duyệt tất cả các vấn đề chính sách có liên quan đến an toàn thông tin và thay đổi nếu có.

- Phê duyệt từng trường hợp ngoại lệ cụ thể nếu như yêu cầu về chính sách an toàn không được đáp ứng, đưa ra khung thời gian cho các trường hợp ngoại lệ và theo dõi các trường hợp này cho tới khi nào đáp ứng được những yêu cầu của chính sách an toàn.

- Tổ chức thảo luận các vấn đề liên quan đến an toàn thông tin và các vấn đề nảy sinh từ các cơ quan, đơn vị để bảo đảm rằng những đơn vị này sẽ nhận được sự tham mưu hữu ích và triển khai các thủ tục bảo vệ an toàn hiệu quả.

- Chỉ đạo và tham mưu cho các đơn vị chịu trách nhiệm xây dựng các hệ thống bảo vệ an toàn.

Chính sách an toàn

Chính sách bảo vệ an toàn chính là bản tuyên ngôn về mục đích quản lý. Cần phải xây dựng một chính sách bảo vệ an toàn toàn diện để làm nền tảng cho việc triển khai các phương án bảo vệ an toàn tại toàn bộ các đơn vị. Chính sách an toàn phải bao trùm toàn bộ các lĩnh vực an toàn thông tin và phải cung cấp các nguyên tắc hướng dẫn cho các đơn vị triển khai các phương án bảo vệ an toàn tại đơn vị của mình.

Dựa trên các tiêu chuẩn an toàn quốc tế, dưới đây là khung đề xuất cho việc xây dựng chính sách an toàn thông tin.

Kiến trúc và các tiêu chuẩn an toàn kỹ thuật

Kiến trúc an toàn kỹ thuật xác định các phương thức bảo vệ an toàn cho nhiều ứng dụng và hợp phần cơ sở hạ tầng. Kiến trúc an toàn thông tin sẽ bao gồm các thông tin đầu vào để xây dựng kiến trúc mạng và ứng dụng bảo đảm tính tương tác về an toàn. Kiến trúc kỹ thuật sẽ đưa ra hướng dẫn về những khía cạnh sau:

Kiến trúc mạng an toàn - Kiến trúc này bao gồm một mạng được thiết kế để bảo đảm cung cấp độ an toàn hợp lý cho từng hợp phần thông qua việc phân chia mạng. Kiến trúc mạng an toàn cũng tính đến các quy định bảo mật khi đưa các dịch vụ lên mạng Internet và sự phân chia mạng giữa các cơ quan và dịch vụ khác nhau. Bên cạnh đó kiến trúc mạng an toàn sẽ bảo đảm các dịch vụ dùng chung như DNS, thư mục và mạng tin cậy được cung cấp một cách an toàn cho tất cả các cơ quan.

Kiến trúc mạng an toàn cũng xác định các thiết bị an toàn và kịch bản triển khai những thiết bị này nhằm bảo vệ cơ sở hạ tầng quan trọng. Các thiết bị an toàn bao gồm thiết bị lọc gói tin, tường lửa, hệ thống phát hiện và ngăn ngừa thâm nhập và hệ thống giám sát và cảnh báo.

Kiến trúc ứng dụng an toàn - Kiến trúc ứng dụng an toàn xác định các tiêu chuẩn an toàn phải được áp dụng khi xây dựng và kết nối ứng dụng. Kiến trúc này bao gồm các tiêu chuẩn an toàn kết nối, quy định mã hóa giữa các ứng dụng (ví dụ như lớp cổng bảo mật SSL), kênh an toàn, hồ sơ xác thực và cấp quyền trong ứng dụng. Các tiêu chuẩn an toàn xuất phát từ chính sách an toàn và đưa ra cái nhìn toàn cảnh về những hành động cần thiết nhằm đạt được các mục tiêu đã đề ra trong chính sách an toàn. Tỉnh Bình Phước cần tập trung xác định các tiêu chuẩn an toàn trong đó cung cấp các hướng dẫn trong việc thực thi chính sách an toàn. Những tiêu chuẩn này bao gồm các quy trình và tiêu chuẩn cụ thể được thiết lập tại toàn bộ các cơ quan nhằm tuân thủ chính sách an toàn. Các tiêu chuẩn cho việc lập cấu hình bảo vệ an toàn của hệ điều hành, các thiết bị mạng và các hợp phần được mua bên ngoài cũng sẽ được xác định một cách tập trung.

2.7.2 Các hợp phần của chính sách ATTT

Phần	Lĩnh vực
1	**Phân loại và kiểm soát thông tin**
1.1	Chủ sở hữu dữ liệu
1.2	Phân loại thông tin
2	**Bảo mật vật lý và môi trường hệ thống**
2.1	An toàn vật lý
2.2	An toàn môi trường hệ thống
2.3	Cấp điện
2.4	An toàn hệ thống dây mạng

Phần	Lĩnh vực
2.5	An toàn máy tính xách tay
2.6	Chính sách dọn bàn làm việc và khoá màn hình
3	**Bảo mật nguồn nhân lực**
3.1	An toàn trong việc tuyển dụng, luân chuyển và chấm dứt hợp đồng lao động
3.2	Trách nhiệm của người sử dụng
3.3	Các khoá học định hướng và nâng cao nhận thức về An toàn
4	**Kiểm soát truy cập logic**
4.1	Quản lý truy nhập của người dùng
4.2	Trách nhiệm của người dùng
4.3	Bảo mật lôgic máy tính cá nhân, máy xách tay
4.4	Quy định sử dụng các tiện ích hệ thống nhạy cảm
5	**Quản trị môi trường máy tính**
5.1	Xác định thiết bị phần cứng
5.2	Xử lý và bảo vệ an toàn thông tin
5.3	Các thủ tục trong tình huống khẩn cấp, các tài khoản ưu tiên
5.4	Thủ tục xử lý tai nạn
5.5	Phân chia trách nhiệm
5.6	Bảo vệ an toàn tài liệu hệ thống
5.7	Kiểm soát virus máy tính
5.8	Thủ tục loại bỏ phương tiện lưu trữ
5.9	Mã hoá và quản lý khoá
6	**An toàn hệ thống mạng**
6.1	Kiểm soát quản lý mạng
6.2	Các thiết bị mạng
6.3	Các công cụ chẩn đoán mạng
7	**An toàn Internet**
7.1	Sử dụng Internet
7.2	An toàn e-mail
7.3	An toàn tường lửa

Phần	Lĩnh vực
8	**Xây dựng và duy trì hệ thống**
8.1	Kiểm soát môi trường hệ thống
8.2	Yêu cầu thay đổi
8.3	Quản lý mã nguồn
8.4	Kiểm soát phiên bản
8.5	Kiểm thử
8.6	Yêu cầu duy trì
8.7	Kỹ thuật dịch ngược
9	**Kế hoạch tiếp tục hoạt động sau thảm hoạ[1]**
9.1	Kế hoạch phục hồi sau thảm hoạ
9.2	Thủ tục sao lưu và phục hồi
10	**Tuân thủ**
10.1	Việc sử dụng phần mềm không được phép
10.2	Mua sắm và quy định sử dụng phần mềm
11	**Bên thứ ba và dịch vụ gia công**
11.1	Đánh giá rủi ro
11.2	Kiểm soát truy cập
11.3	Các điều kiện bảo mật trong hợp đồng với bên thứ ba
11.4	Các điều kiện bảo mật trong các hợp đồng gia công
11.5	Cam kết chất lượng dịch vụ

Các hợp phần của chính sách bảo mật

Các dịch vụ bảo mật như được minh họa trong hình dưới đây, là tập hợp các công nghệ cung cấp khung kiểm soát bảo mật cho tất cả các công nghệ trong các vùng dịch vụ khác.

[1] Kế hoạch tiếp tục hoạt động sau thảm hoạ cần phải được triển khai cho chương trình CPĐT nhằm bảo đảm khả năng sẵn sàng 24X7 của cơ sở hạ tầng và dịch vụ CPĐT.

- Kiểm soát danh tính và truy cập: Kiểm soát danh tính và truy cập là một vùng quản trị rộng có chức năng xác định các cá nhân trong một hệ thống (ví dụ quốc gia, hệ thống mạng, tổ chức của cá nhân đó) và kiểm soát truy cập vào các nguồn lực trong hệ thống này bằng cách đặt ra những giới hạn về danh tính đã thiết lập cho các cá nhân đó.

  - Quản lý danh tính: Quản lý danh tính là một nền tảng phần mềm quản lý phương thức người dùng được xác định và ủy quyền thông qua các hệ thống mạng máy tính. Quản lý danh tính bao gồm các vấn đề như cách thức người dùng được gán một danh tính, bảo vệ danh tính đó và các công nghệ hỗ trợ việc bảo vệ đó.
  - Xác thực: Xác thực là giao thức bảo mật được sử dụng để xác nhận danh tính của một thực thể trước khi đưa thực thể đó đến kiểm tra ủy quyền trong một hệ thống kiểm soát truy cập.
    - Kerberos: Là giao thức xác thực mạng máy tính hoạt động trên cơ sở "vé" để cho phép các nút mạng trao đổi thông tin thông qua một đường truyền không an toàn

nhằm chứng minh danh tính của các nút mạng đó với các nút mạng khác theo phương thức an toàn. Mục tiêu khi thiết kế giao thức này là nhằm vào mô hình khách - chủ và đảm bảo xác thực cho cả hai chiều - cả người dùng và máy chủ đều xác nhận được danh tính của nhau. Thông điệp của giao thức Kerberos được bảo vệ chống lại việc nghe lén và gửi lại các gói tin cũ. Kerberos xây dựng dựa trên mật mã hóa khóa đối xứng và cần đến một bên thứ ba được tin tưởng, và tùy ý có thể sử dụng mật mã hóa khóa công khai bằng cách tận dụng mật mã hóa khóa không đối xứng trong các giai đoạn chứng thực nhất định.

- Remote Authentication Dial In User Service (RADIUS): Là giao thức mạng cung cấp quản lý AAA (Xác thực, Phân quyền và Tính cước) tập trung cho máy tính để kết nối và sử dụng dịch vụ mạng. RADIUS được phát triển bởi Tập đoàn Livingston Enterprises vào năm 1991 như một giao thức xác thực và tính cước cho máy chủ truy cập và sau đó được đưa vào tiêu chuẩn Internet Engineering Task Force (IETF).

- Kiểm soát truy cập: Kiểm soát truy cập là một hệ thống cho phép xác thực để kiểm soát truy cập trong các khu vực và nguồn lực của một cơ sở vật lý hoặc một hệ thống thông tin dựa trên máy tính. Một số ví dụ về kiểm soát truy cập:
  - Firewall: Thiết bị được thiết kế để cho phép hoặc từ chối truyền mạng dựa trên một số nguyên tắc và thường được sử dụng để bảo vệ hệ thống mạng khỏi các truy cập trái phép trong khi đó những trao đổi thông tin hợp pháp vẫn được thông qua.
  - Network Access Control (NAC): phương thức bảo mật mạng lưới máy tính hợp nhất các công nghệ bảo mật điểm đầu nút (ví dụ như antivirus, ngăn chặn xâm nhập và lỗ hổng máy chủ), xác thực người dùng hoặc hệ thống và thực hiện bảo mật đường truyền.

- Kiểm định: Kiểm định chỉ một bản ghi các hoạt động trong hệ thống theo thứ tự thời gian cho phép kiểm tra và tái thiết lập trình tự các sự kiện và/ hoặc các thay đổi trong một sự kiện; thu thập, chuẩn hóa và phân tích các nhật ký từ các thiết bị trên toàn hệ thống mạng, ví dụ như các nhật ký từ tường lửa, các hệ thống phát hiện và ngăn chặn xâm nhập và các giải pháp chống mất dữ liệu cũng như lưu lượng truy cập mạng, các nhật ký ứng dụng và hoạt động của người dùng.

- Kiểm soát đe dọa và xâm nhập: Kiểm soát đe dọa và xâm nhập là nền tảng được sử dụng để ngăn chặn sự xuất hiện của những sự cố bảo mật bằng cách kiểm soát sự đe dọa cũng như các xâm nhập đến bảo mật.

- Quản lý xâm nhập: Quản lý xâm nhập là nền tảng phần mềm được sử dụng để phát hiện và hạn chế những xâm nhập/lỗ hổng phát hiện trong hệ thống mạng máy tính, đảm bảo khả năng quét lỗ hổng và bản vá xác thực, công cụ này xác định các chương trình đã cài đặt và các bản vá (patches) bảo mật còn thiếu.
- Quản lý đe dọa: Quản lý đe dọa là nền tảng phần mềm được sử dụng để phát hiện và ngăn chặn các đe dọa bảo mật ví dụ như sự tấn công chủ động đến các hệ thống được bảo vệ.

- Hệ thống Antivirus: là gói phần mềm được sử dụng để ngăn chặn, phát hiện và hủy phần mềm độc hại (malware), bao gồm nhưng không giới hạn virus máy tính, sâu máy tính, trojan horses, spyware và adware.
- Hệ thống ngăn chặn xâm nhập: thường là các thiết bị bảo mật đường truyền có chức năng giám sát mạng và/ hoặc các hoạt động trong hệ thống để xác định các hoạt động nguy hiểm. Chức năng chính của hệ thống ngăn chặn xâm nhập là xác định các hoạt động nguy hiểm, thông tin đăng nhập của các hoạt động đó, cố gắng ngăn chặn/ dừng hoạt động và đưa ra cảnh báo về các hoạt động đó.
- Hệ thống quản lý sự kiện và thông tin bảo mật (Security event and information manager - SIEM): là một công cụ máy tính được sử dụng trên các đường truyền dữ liệu để tập trung kho lưu trữ và giải thích các bản ghi hoặc sự kiện bảo mật được tạo ra bởi các phần mềm khác chạy trong hệ thống mạng. SIEM thường thực hiện sự tương quan và giải thích về các bản ghi đã thu thập, và chỉ định nguy cơ và/hoặc mức tin cậy nhằm giúp giảm các cảnh báo sai tích cực (false-positive).

- Kiểm soát tính bảo mật và tính toàn vẹn: Kiểm soát tính bảo mật và tính toàn vẹn đề cập đến các nền tảng và công nghệ được sử dụng để bảo vệ tính bảo mật và xác thực của thông tin.

- Nền tảng PKI: Nền tảng PKI (Cơ sở hạ tầng khóa công khai) là nền tảng phần mềm cho phép tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi chứng thực số. Trong mật mã, PKI là sự sắp xếp các khóa công khai liên kết với người dùng tương ứng bằng các phương tiện của nhà cung cấp chứng thực (CA).
- Mã hóa mạng: Mã hóa mạng là phương pháp duy trì tính bảo mật và tính toàn vẹn của thông tin được trao đổi trên hệ thống mạng hoặc tại tầng giao vận. Một số ví dụ về mã hóa mạng:
  - Internet Protocol Security (IPsec): bộ giao thức bảo đảm trao đổi thông tin trên Giao thức Internet bằng cách xác thực và mã hóa mỗi gói IP của một kỳ trao đổi thông tin. IPsec cũng bao gồm các giao thức thiết lập xác thực hai chiều giữa các tác nhân tại đầu kỳ trao đổi và thương thảo khóa mật mã được sử dụng trong suốt kỳ trao đổi đó.
  - OpenVPN: là ứng dụng phần mềm mã nguồn mở miễn phí thực hiện kỹ thuật mạng riêng ảo (VPN) để tạo kết nối điểm-tới-điểm hoặc site-to-site trong các cấu hình định tuyến hoặc bắc cầu và các phương tiện truy cập từ xa. OpenVNP sử dụng phương pháp bảo mật SSL/TLS để mã hóa và có khả năng vượt qua công nghệ chuyển dịch địa chỉ mạng (NATs) và tường lửa.
- Mã hóa kho lưu trữ: Mã hóa kho lưu trữ là phương pháp duy trì tính bảo mật và tính toàn vẹn của thông tin được lưu trữ, ví dụ như tập tin và/ hoặc cơ sở dữ liệu. Một số ví dụ về mã hóa kho lưu trữ:
  - Mã hóa ổ đĩa cứng sử dụng phần mềm hoặc phần cứng mã hóa ổ đĩa để mã hóa mọi bit dữ liệu ghi trên đĩa, hoặc khối lượng đĩa. Mã hóa ổ đĩa ngăn chặn truy cập trái phép vào kho lưu trữ dữ liệu. Thuật ngữ "mã hóa toàn bộ ổ đĩa cứng"

(full disk encryption hoặc whole disk encryption) thường được sử dụng để nhấn mạnh rằng mọi dữ liệu trên đĩa đã được mã hóa, bao gồm cả các chương trình mã hóa phân vùng hệ điều hành khởi động.

- Mã hóa hệ thống tệp tin, thường được gọi là mã hóa tệp tin hoặc thư mục, là một hình thức mã hóa ổ đĩa cứng mà trong đó các tệp tin hoặc thư mục riêng biệt được mã hóa bởi chính hệ thống tệp tin của riêng mình. Điều này đối lập với mã hóa toàn bộ ổ đĩa cứng khi mà toàn bộ phân vùng hoặc ổ đĩa cứng chứa hệ thống tệp tin được mã hóa.

- Kiểm chuẩn tính toàn vẹn: Kiểm chuẩn tính toàn vẹn là phương pháp chứng thực tính toàn vẹn của hệ thống thông tin và dữ liệu. Kiểm chuẩn tính toàn vẹn của tệp tin là quá trình sử dụng một thuật toán để xác minh tính toàn vẹn hoặc tính xác thực của một tập tin máy tính. Điều này thường được thực hiện bằng cách so sánh hàm băm mật mã học (cryptographic hash function) của các tập tin so với một tài liệu tham chiếu đã biết. Một số phương pháp kiểm chuẩn tính toàn vẹn:

  - SHA-1: là một hàm băm mật mã học được xây dựng bởi Cơ quan An ninh Quốc gia (National Security Agency) và được phát hành bởi NIST theo Tiêu chuẩn Xử lý Thông tin của Liên Bang Hoa Kỳ (U.S. Federal Information Processing Standard). SHA là viết tắt của Thuật toán giải Băm An toàn (Secure Hash Algorithm). Ba thuật toán SHA được kết cấu khác nhau và được phân biệt bằng các tên gọi SHA-0, SHA-1, và SHA-2. SHA-1 rất giống với SHA-0 nhưng SHA-1 sửa một lỗi trong đặc điểm kỹ thuật băm SHA gốc, mà lỗi này là nguồn gốc dẫn đến những điểm yếu đáng kể. Nhiều ứng dụng không chấp nhận thuật toán SHA-0.
  - MD5 (Message-Digest algorithm 5): một hàm băm mật mã học được sử dụng phổ biến với giá trị băm dài 128-bit (16-byte). Là một chuẩn Internet (RFC1321), MD5 đã được dùng trong nhiều ứng dụng bảo mật, và cũng được dùng phổ biến để kiểm tra tính toàn vẹn của dữ liệu. Tuy nhiên, người ta đã chứng minh rằng MD5 không có khả năng chịu va chạm, như vậy, MD5 là không phù hợp cho các ứng dụng như giấy chứng nhận SSL (SSL certificates) hoặc chữ ký số (digital signatures) dựa trên thuộc tính này. Một bảng băm MD5 thường được diễn tả bằng một số hệ thập lục phân 32 ký tự.

2.7.3 Các yêu cầu đảm bảo ATTT của tỉnh

Việc triển khai mô hình đảm bảo ATTT của tỉnh Bình Phước cần đáp ứng các yêu cầu sau:

- Các yêu cầu đảm bảo an toàn mức vật lý

  - Các khu vực sau phải được kiểm soát truy cập vật lý để phòng tránhtruy cập trái phép hoặc sai mục đích: Trung tâm dữ liệu, khu vực chứa máy chủ và thiết bị lưu trữ, các tủ mạng và đấu nối, thiết bị nguồn điện và dự phòng điện khẩn cấp, các phòng vận hành, kiểm soát (quản trị) hệ thống. Đơn vị quản lý các vùng thiết bị trên phải có nội quy hoặc hướng dẫn làm việc trong các khu vực này.

- Người dùng sử dụng các thiết bị lưu trữ dữ liệu di động (máy tính xách tay, thiết bị số cầm tay, thẻ nhớ USB, ổ cứng ngoài, băng từ...) để lưu thông tin thuộc phạm vi bảo vệ theo quy định có trách nhiệm bảo vệ các thiết bị này và thông tin lưu trên thiết bị, tránh làm mất, lộ thông tin.
- Không mang ra nước ngoài thông tin của cơ quan, Nhà nước không liên quan tới nội dung công việc thực hiện ở nước ngoài. Nghiêm cấm sử dụng thiết bị do cá nhân tự trang bị để lưu giữ bí mật Nhà nước.
- Các thiết bị lưu trữ không sử dụng tiếp cho công việc của đơn vị (thanh lý, cho, tặng) phải được xoá nội dung bằng phần mềm hoặc bằng thiết bị hủy dữ liệu chuyên dụng hay phá hủy vật lý.

- Các yêu cầu đảm bảo an toàn máy tính làm việc
  - Máy tính phục vụ công việc (bao gồm máy chủ, máy quản trị và máy tính phục vụ công việc của người dùng tại đơn vị):
    - Máy tính làm việc chỉ được cài đặt phần mềm theo danh mục phần mềm do đơn vị quy định và do bộ phận công nghệ thông tin của đơn vị quản lý hoặc được cung cấp theo các chương trình ứng dụng công nghệ thông tin của tỉnh hoặc các cơ quan Nhà nước khác có thẩm quyền, được cập nhật bản vá lỗi hệ điều hành về an ninh, cài đặt phần mềm phòng diệt virus và cập nhật mẫu phát hiện virus gần nhất.
    - Bộ phận công nghệ thông tin của đơn vị chịu trách nhiệm cài đặt phần mềm cho máy tính phục vụ công việc. Người dùng không được can thiệp (cài đặt mới, thay đổi, gỡ bỏ,…) các phần mềm đã cài đặt trên máy tính khi chưa được sự đồng ý của bộ phận công nghệ thông tin của đơn vị.
    - Người dùng phải thực hiện thao tác khoá máy tính (sử dụng tính năng cài đặt sẵn trên máy) khi rời khỏi nơi đặt máy tính và tắt máy tính khi rời khỏi cơ quan.
  - Máy tính do cá nhân tự trang bị phải đáp ứng đầy đủ các điều kiện dưới đây khi kết nối vào hệ thống mạng nội bộ:
    - Cài đặt đầy đủ các bản vá lỗi hệ điều hành về an ninh.
    - Cài đặt phần mềm phòng diệt mã độc và cập nhật mẫu mã độc gần nhất.
    - Không cài đặt phần mềm, công cụ có tính năng gây mất an toàn thông tin hoặc tạo rủi ro cho hệ thống mạng (cấp phát địa chỉ mạng, dò quét mật khẩu, dò quét cổng mạng, giả lập tấn công,..).

- Các yêu cầu về đảm bảo an toàn hệ thống mạng máy tính
  - Kết nối mạng diện rộng phải được thiết lập và vận hành theo yêu cầu quản lý, vận hành và sử dụng hạ tầng truyền thông thống nhất của tỉnh.
  - Phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập và kiểm soát truy cập giữa các vùng bằng tường lửa.
  - Mạng nội bộ của các cơ quan, đơn vị QLNN phải đảm bảo phân chia tối thiểu thành

các vùng mạng trong và vùng mạng ngoài.

- Vô hiệu hoá tất cả các dịch vụ không sử dụng tại từng vùng mạng;
- Che giấu và tránh truy cập trực tiếp các địa chỉ mạng bên trong từ bên ngoài (Internet và hạ tầng truyền thông của Tỉnh)
- Cài đặt các bản cập nhật, vá lỗi đúng hạn cho các tường lửa để khắc phục các điểm yếu an ninh nghiêm trọng; Có chế độ bảo hành hoặc thiết bị dự phòng để đảm bảo sự hoạt động liên tục của tường lửa.

- Mạng nội bộ của cơ quan và các đơn vị QLNN trên địa bàn tỉnh phải được giám sát bởi hệ thống phát hiện và phòng chống tấn công.

- Hệ thống mạng không dây (nếu có) phải đáp ứng các điều kiện tối thiểu sau:
  - Các thiết bị phần cứng phải có chứng nhận hợp quy theo quy định;
  - Áp dụng mã hoá dữ liệu truyền nhận sử dụng thuật toán mã hoá an toàn;
  - Người dùng không dây phải được cung cấp định danh duy nhất và xác thực qua kênh mã hoá.
  - Các điểm truy cập không dây (thiết bị phát sóng làm cầu nối giữa mạng có dây và không dây) của đơn vị được bảo vệ tránh bị tiếp cận trái phép
- Đối với truy cập từ xa vào hệ thống mạng nội bộ:
  - Máy tính dùng để kết nối tới mạng của đơn vị phải được đảm bảo ATTT.
  - Kết nối truy cập từ xa phải sử dụng mã hóa kênh truyền theo tiêu chuẩn mã hóa do Bộ Thông tin và Truyền thông quy định.
  - Các truy cập từ xa cho mục đích quản trị hệ thống phải áp dụng xác thực tối thiểu 2 yếu tố.
  - Hạn chế truy cập từ xa vào mạng nội bộ từ những điểm truy cập Internet công cộng.
- Các yêu cầu đảm bảo an toàn kết nối Internet:
  - Các Đơn vị áp dụng các biện pháp cần thiết để đảm bảo an toàn thông tin trong hoạt động kết nối Internet, tối thiểu đáp ứng yêu cầu sau:
    - Có tường lửa kiểm soát truy cập Internet.
    - Lọc bỏ, không cho phép truy cập các trang tin có nghi ngờ chứa mã độc hoặc các nội dung không phù hợp (phản động hoặc trái thuần phong mỹ tục).
    - Không mở trang tin hoặc ứng dụng Internet ngay trên máy tính chứa dữ liệu quan trọng hoặc có khả năng tiếp cận các dữ liệu, ứng dụng quan trọng của tỉnh. Trường hợp cần thiết chỉ được truy cập vào các trang tin trên Internet phục vụ công việc của đơn vị.
    - Xác định, phân loại các loại dữ liệu và ứng dụng quan trọng trên hệ thống mạng nội bộ cần được bảo vệ trong kết nối Internet.
  - Kết nối Internet cho máy tính phục vụ công việc của người dùng tại đơn vị bị thu hẹp phạm vi hoặc bị ngắt trong các trường hợp sau:

- Có chỉ đạo yêu cầu thu hẹp phạm vi kết nối Internet hoặc ngắt kết nối Internet (áp dụng trong các trường hợp khẩn cấp).
- Lãnh đạo đơn vị quyết định hạn chế phạm vi kết nối hoặc ngắt hoàn toàn kết nối Internet máy tính phục vụ công việc của người dùng để đảm bảo an toàn cho hệ thống mạng của đơn vị và hạn chế các ảnh hưởng khác của Internet tới hoạt động của đơn vị.

o Đối với máy chủ và thiết bị công nghệ thông tin khác, chỉ thiết lập kết nối Internet cho các hệ thống cần phải có giao tiếp với Internet (các máy chủ, thiết bị cung cấp giao diện ra Internet của trang tin điện tử, thư điện tử; thiết bị cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công).

- Các yêu cầu đảm bảo an toàn mức ứng dụng:

o Yêu cầu về đảm bảo ATTT phải được đưa vào tất cả các công đoạn liên quan đến ứng dụng (thiết kế, xây dựng, triển khai và vận hành, sử dụng).

o Ứng dụng do đơn vị phát triển hoặc thuê phát triển phải đáp ứng yêu cầu:

- Mã hóa thông tin bí mật hoặc nhạy cảm.
- Kiểm tra tính hợp lệ của dữ liệu đầu vào và đầu ra để đảm bảo dữ liệu chính xác và phù hợp.
- Giới hạn số lần đăng nhập sai liên tiếp vào ứng dụng.
- Thực hiện quy trình kiểm soát việc cài đặt phần mềm trên các máy chủ, máy tính của người dùng, thiết bị mạng đang hoạt động thuộc hệ thống mạng nội bộ, đảm bảo các phần mềm khi cài đặt trong hệ thống có nguồn gốc an toàn, không bị nhiễm mã độc.
- Hạn chế truy cập tới mã nguồn chương trình và phải đặt mã nguồn trong môi trường an toàn do bộ phận chuyên trách quản lý.
- Kiểm tra phát hiện và khắc phục điểm yếu của ứng dụng trước khi đưa vào sử dụng và trong quá trình sử dụng.

o Đối với phần mềm bản quyền, phần mềm thương mại hoặc đóng gói:

- Theo dõi, nắm bắt thông tin về các điểm yếu được phát hiện và cập nhật thường xuyên bản vá lỗi về an ninh cho ứng dụng.
- Trường hợp điểm yếu đã được phát hiện mà chưa có bản vá lỗi của đơn vị sản xuất phần mềm, phải thực hiện đánh giá rủi ro và có biện pháp phòng tránh phù hợp.

- Các yêu cầu đảm bảo an toàn mức dữ liệu:

o Nội dung mật, quan trọng hoặc nhạy cảm khi lưu trữ trên thiết bị di động hoặc truyền nhận trên hệ thống mạng phải được mã hóa, trong đó:

- Các bí mật nhà nước phải được mã hóa bằng giải pháp do Ban Cơ yếu Chính phủ cung cấp hoặc được cấp có thẩm quyền chấp nhận sử dụng trên địa bàn tỉnh.

- Áp dụng mã hóa kênh kết nối cho các hoạt động sau theo tiêu chuẩn mã hóa do Bộ Thông tin và Truyền thông quy định: quản trị hệ thống; đăng nhập mạng, ứng dụng; gửi nhận dữ liệu tự động giữa các máy chủ; nhập và biên tập dữ liệu; tra cứu dữ liệu mật, nhạy cảm.
- Khuyến khích áp dụng công nghệ chữ ký số để xác thực và bảo mật dữ liệu, đặc biệt trong trường hợp cần đảm bảo chống từ chối nguồn gốc dữ liệu.
- Văn bản điện tử có nội dung cần hạn chế tiếp cận nhưng không thuộc danh mục bí mật Nhà nước được sử dụng tính năng mã hóa (đặt mật khẩu) của các ứng dụng văn phòng (phần mềm soạn thảo, đọc văn bản, nén tệp), nhưng phải sử dụng thuật toán mã hóa an toàn.

o Cá nhân thực hiện soạn thảo, gửi, nhận dữ liệu có trách nhiệm xác định mức độ mật, nhạy cảm của dữ liệu để thực hiện phương thức bảo vệ dữ liệu phù hợp hoặc yêu cầu bộ phận công nghệ thông tin hướng dẫn, hỗ trợ phương thức bảo vệ trong trường hợp cần thiết.

o Chỉ sử dụng hệ thống thư điện tử và các công cụ trao đổi thông tin do đơn vị quản lý trực tiếp, hoặc các CQNN, các tổ chức có thẩm quyền cung cấp để trao đổi thông tin, tài liệu làm việc. Không sử dụng các phương tiện trao đổi thông tin công cộng trên Internet cho mục đích này.

- Các yêu cầu đảm bảo ATTT trong hoạt động trao đổi thông tin với các tổ chức, cá nhân bên ngoài:

o Tổ chức, cá nhân tham gia hệ thống phải cam kết bảo mật thông mà tổ chức, cá nhân đó sẽ tiếp xúc trước khi bắt đầu thực hiện công việc theo hợp đồng, thỏa thuận giữa hai bên.

o Khi trao đổi các thông tin cần bảo mật qua hệ thống mạng phải mã hóa theo quy định. Khi trao đổi bí mật nhà nước phải thực hiện theo quy định về công tác bảo vệ bí mật nhà nước của tỉnh.

o Đối với tổ chức, cá nhân bên ngoài có thiết lập kết nối vào mạng nội bộ:

- Phải phân tích rủi ro về an toàn thông tin trước khi kết nối mạng và có biện pháp kiểm soát các rủi ro này.
- Thỏa thuận bằng văn bản giữa các bên về các điều kiện cụ thể mà tổ chức, cá nhân bên ngoài phải đáp ứng khi kết nối vào mạng nội bộ; kiểm tra định kỳ việc thực hiện thỏa thuận này.
- Điều kiện tổ chức, cá nhân bên ngoài phải đáp ứng tối thiểu bao gồm: vùng mạng của tổ chức, cá nhân bên ngoài được sử dụng để kết nối vào mạng nội bộ phải được kiểm soát bằng tường lửa; các máy tính trong phân đoạn mạng này phải được cập nhật bản vá hệ điều hành, mẫu phòng diệt mã độc; các tài khoản truy cập hệ thống tối thiểu phải áp dụng mật khẩu phức tạp; chỉ được kết nối Internet trong trường hợp kết nối này phục vụ công việc nội bộ.

- Đối tác phát triển ứng dụng cho các cơ quan, đơn vị trên địa bàn tỉnh có trách nhiệm đảm bảo an toàn cho công tác phát triển ứng dụng, bao gồm cả giai đoạn bảo trì, bảo hành ứng dụng: sử dụng máy tính được cập nhật bản vá hệ điều hành, phần mềm phòng diệt mã độc; thực hiện các biện pháp tránh lộ lọt mã nguồn, phần mềm ứng dụng nội bộ và các tài liệu liên quan.

- Các yêu cầu về đảm bảo Sao lưu, dự phòng sự cố:
  - Đơn vị phải có thiết bị, quy trình, nhân sự phục vụ công tác sao lưu dữ liệu phòng ngừa sự cố; định kỳ kiểm tra dữ liệu sao lưu và phục hồi thử hệ thống từ dữ liệu sao lưu; quản lý, bảo quản phương tiện sao lưu phòng tránh hỏng, mất dữ liệu sao lưu.
  - Đối với hệ thống quan trọng, đơn vị phải có biện pháp dự phòng về thiết bị, phần mềm để đảm bảo sự hoạt động liên tục của hệ thống.
- Các yêu cầu về đảm bảo ATTT cho tài khoản công nghệ thông tin:
  - Tài khoản người dùng:
    - Mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị phải có cơ chế xác định các cá nhân có trách nhiệm quản lý tài khoản.
    - Tài khoản của người dùng không được có quyền quản trị trên máy tính nối mạng. Tài khoản quản trị máy tính chỉ được sử dụng trong trường hợp cài đặt phần mềm trên máy tính. Tài khoản quản trị máy tính để bàn phải do bộ phận công nghệ thông tin của đơn vị nắm giữ. Đối với máy tính xách tay, người dùng phải được hướng dẫn sử dụng đúng cách tài khoản quản trị máy tính và có trách nhiệm thực hiện theo đúng hướng dẫn.
    - Trường hợp người dùng thay đổi vị trí công tác, chuyển công tác, thôi việc hoặc nghỉ hưu phải thông báo kịp thời cho bộ phận quản lý tài khoản công nghệ thông tin để thực hiện điều chỉnh, thu hồi, hủy bỏ các quyền sử dụng của người dùng đối với hệ thống mạng, ứng dụng.
  - Tài khoản quản trị hệ thống (thiết bị, mạng, hệ điều hành, ứng dụng, cơ sở dữ liệu) phải tách biệt với tài khoản truy cập mạng, ứng dụng với tư cách người dùng thông thường. Tài khoản quản trị hệ thống phải được giao đích danh cá nhân làm công tác quản trị hệ thống. Hạn chế dùng chung tài khoản quản trị.
  - Phương tiện xác thực tài khoản:
    - Mật khẩu phức tạp phải được áp dụng cho tất cả các tài khoản truy cập, sử dụng, quản trị hệ thống.
    - Đổi mật khẩu ngay sau khi nhận bàn giao từ người khác hoặc có thông báo về sự cố ATTT, điểm yếu liên quan đến khả năng lộ mật khẩu; đổi mật khẩu tối thiểu 03 tháng một lần đối với tài khoản của người dùng và 02 tháng một lần đối với tài khoản quản trị hệ thống.

- Người dùng, người làm công tác quản trị hệ thống có trách nhiệm bảo vệ thông tin tài khoản được cấp.

- Rà soát tối thiểu mỗi năm một lần các tài khoản đang cấp trên hệ thống, đảm bảo các tài khoản và quyền truy cập hệ thống được cấp phát đúng.

- Đảm bảo an toàn trong công tác quản trị hệ thống

- Quản trị hệ thống:
  - Máy tính dùng để quản trị hệ thống chỉ được cài đặt phần mềm cần thiết cho hoạt động quản trị hệ thống, đặt trong vùng mạng phục vụ công tác quản trị hệ thống và chỉ được cấp quyền truy cập cho các cá nhân được giao trách nhiệm quản trị hệ thống.
  - Đổi tên tài khoản mặc định (nếu có thể) và mật khẩu mặc định của quản trị hệ thống khi hệ thống được thiết lập.
  - Sử dụng kênh trao đổi thông tin an toàn (có mã hóa) cho truy cập quản trị hệ thống.
- Thực hiện quản lý cấu hình hệ thống quan trọng: Quản lý thông tin về thông số kỹ thuật, mục đích sử dụng, vị trí lắp đặt, nguồn cung cấp, thời gian sử dụng, bảo hành, bảo dưỡng; đảm bảo thông tin sẵn dụng khi có yêu cầu (phục vụ công tác đánh giá năng lực, tính sẵn sàng, an toàn của hệ thống, công tác mua sắm, bảo dưỡng, bảo hành).
- Thực hiện quản lý thay đổi đối với hệ thống quan trọng: Xác định mức độ cần thiết của thay đổi, ảnh hưởng tiềm ẩn (các sự cố có thể xảy ra, phạm vi tác động) và biện pháp phòng tránh (bao gồm thủ tục hủy bỏ thay đổi và khôi phục hệ thống khi thay đổi không thành công), xác định thời gian thực hiện phù hợp; phê duyệt kế hoạch thay đổi; thông báo cho các bên liên quan về kế hoạch và kết quả của thay đổi.
- Thực hiện quản lý năng lực hệ thống quan trọng: Giám sát hiệu năng và thực hiện các biện pháp cần thiết (dọn dẹp hệ thống, điều chỉnh thông số kỹ thuật, bổ sung mua sắm) để đảm bảo khả năng xử lý và tính sẵn sàng của hệ thống theo yêu cầu.
- Kiểm tra, đảm bảo nhật ký hệ thống của các thành phần thuộc hệ thống quan trọng được lưu liên tục tối thiểu trong 03 tháng gần nhất và sẵn sàng sử dụng cho công tác phân tích sự cố an toàn thông tin.

- Các yêu cầu về đảm bảo quản lý an toàn thông tin

- Đơn vị phải phân công nhân sự quản lý an toàn thông tin trên môi trường máy tính và mạng máy tính (bao gồm công tác giám sát, kiểm tra việc thực hiện quy định này tại đơn vị).
- Các hệ thống an ninh mạng (cập nhật bản vá hệ điều hành, phòng diệt mã độc, tường lửa, phát hiện và phòng chống tấn công,...) phải được giám sát thường xuyên để đảm bảo tác dụng của hệ thống, đồng thời phát hiện và xử lý sớm các vấn đề về an toàn thông tin. Thực hiện kết xuất định kỳ hàng tháng hoặc hàng quý các báo cáo từ hệ

thống an ninh mạng để theo dõi, đánh giá các vấn đề của hệ thống.

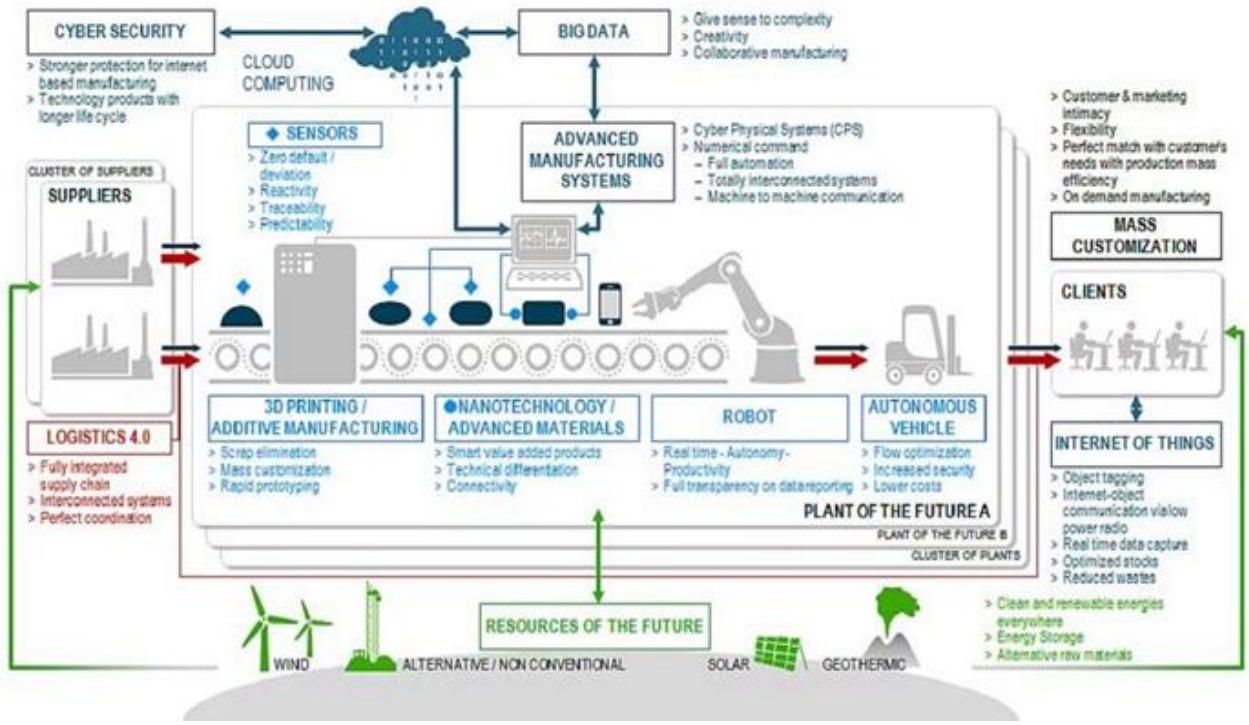
- Thực hiện quản lý rủi ro an toàn thông tin: Xác định các rủi ro an toàn thông tin đối với thông tin, dữ liệu và các hệ thống quan trọng của đơn vị; phân tích, đánh giá các rủi ro này và nghiên cứu, triển khai các biện pháp khắc phục phù hợp. Thực hiện công tác này mỗi khi đơn vị có thay đổi về nhu cầu bảo vệ thông tin, thay đổi trong hệ thống công nghệ thông tin của đơn vị hoặc khi xuất hiện các nguy cơ mất an toàn thông tin mới hoặc tối thiểu mỗi năm một lần.
- Thực hiện quản lý sự cố an toàn thông tin: Thiết lập quy trình báo cáo sự cố an toàn thông tin cho các cấp quản lý thuộc đơn vị; phân tích, xác định nguyên nhân của sự cố, biện pháp khắc phục và ngăn ngừa tái diễn; tổng hợp thông tin về các sự cố trong báo cáo an toàn thông tin định kỳ của đơn vị.
- Người dùng phải được bộ phận công nghệ thông tin của đơn vị hướng dẫn, hỗ trợ, cung cấp các công cụ cần thiết để thực hiện trách nhiệm đảm bảo an toàn thông tin theo quy định.

3. Hệ thống Chính quyền điện tử trong Đô thị thông minh

Giới thiệu về Đô thị thông minh

Đô thị thông minh (Smart City) được xây dựng dựa trên viễn cảnh về sự phát triển đô thị trong tương lai được đánh dấu bởi sự số hóa trên quy mô rộng lớn các loại hình dịch vụ, với mục tiêu chủ yếu là đạt tính bền vững kép trên cả ba phạm vi là kinh tế, xã hội và môi trường, có sử dụng các công nghệ tiên tiến như công nghệ thông tin, công nghệ truyền thông và mạng Internet. Bên cạnh đí, Đô thị thông minh coi trọng sự mở rộng không ngừng của việc cung cấp dữ liệu, góp phần làm đa dạng hóa cách thức lựa chọn của mỗi công dân đô thị nhằm cải thiện các điều kiện sinh sống và học tập hoặc lao động qua đó có thể phát triển bản thân một cách toàn diện và làm xã hội trở nên thịnh vượng. Việc ứng dụng CNTT trong phát triển Đô thị thông minh là tăng cường, đẩy mạnh việc triển khai các hệ thống, công nghệ số hóa trong tất cả các lĩnh vực hoạt động của mình để đảm bảo chất lượng cuộc sống cũng như tính hiệu quả trong mọi hoạt động.

Hiện nay, xây dựng một Đô thị thông minh được xem như là giải pháp chiến lược để giải quyết các vấn đề phát sinh do sự tăng dân số và đô thị hóa nhanh chóng. Hệ thống của Smart city sử dụng các công nghệ ICT để hỗ trợ việc tổ chức, quản lý tỉnh. Tất cả các hoạt động của các lĩnh vực khác nhau như y tế, giao thông, tài nguyên môi trường, điện lực…đều được thu thập dữ liệu (thông qua các thiết bị cảm biến, máy móc…) để đưa về trung tâm xử lý, hỗ trợ ra quyết định cũng như liên thông dữ liệu với nhau để để đưa ra quyết định xử lý chính xác, hiệu quả. Ví dụ như cảm biến đo độ sáng ngoài trời để quyết định bật đèn đường thay vì cài đặt giờ sẵn như hiện nay, hoặc hệ thống điều phối giao thông dựa trên dữ liệu thu thập được về thời tiết để đưa ra cảnh báo cho người tham gia giao thông.



Mô hình tham chiếu Đô thị thông minh

Đô thị thông minh nhấn mạnh trước hết tính hiệu quả trong ba lĩnh vực then chốt là: 1. Khai thác cơ sở hạ tầng kỹ thuật; 2. Quản lý xã hội; 3. Quá trình học hỏi cũng như sự thích ứng nhanh đối với những thay đổi của điều kiện phát triển, mở rộng ra sáu phạm vi trong cuộc sống đô thị và bao hàm trong đó rất nhiều khía cạnh, cụ thể như sau: 1. Con người thông minh (được hưởng một nền giáo dục tiên tiến, sống trong một xã hội hài hòa tôn trọng tính đa dạng, được tạo điều kiện tốt nhất để phát huy sự sáng tạo của mỗi cá nhân và các giá trị nhân văn cốt lõi được chú trọng), 2. Nền kinh tế thông minh (tập trung đầu tư đổi mới công nghệ và kinh doanh, nâng cao năng suất lao động, thiết lập sự liên kết vùng bên cạnh liên kết toàn cầu), 3. Phương tiện đi lại thông minh (phát triển hệ thống giao thông tích hợp với nhiều hình thức tiếp cận, sử dụng nhiên liệu sạch và khuyến khích giao thông phi cơ giới trong khu ở), 4. Cuộc sống thông minh (đề cao lối sống lành mạnh, hướng tới sự sống động về mặt văn hóa, đảm bảo sự an toàn và chăm lo cho hạnh phúc của người dân), 5. Môi trường thông minh (bao gồm quy hoạch xanh, xây dựng xanh, sử dụng năng lượng sạch và gìn giữ các nguồn tài nguyên thiên nhiên) và 6. Quản lý thông minh (đạt tiêu chuẩn trong việc ra quyết sách phục vụ lợi ích cộng đồng, xây dựng hệ thống luật pháp vững mạnh, kiện toàn hệ thống quản lý và áp dụng quy chế công khai, minh bạch cho thông tin và tất cả các hoạt động).

Các yếu tố cốt lõi để triển khai Smart City

Thứ nhất là cần một hệ thống hạ tầng kỹ thuật công nghệ thông tin và truyền thông (ICT) hiện đại đủ phủ kín tỉnh. Hệ thống ICT đảm bảo của địa phương phải đảm bảo "vạn vật được kết nối" (Internet of Things). Để làm được điều đó, người ta phải sử dụng các thiết bị công nghệ cao (high technical) như các cảm biến đa chủng (sensor), camera, mạng không dây tốc độ cao, các đường truyền cáp quang, xử lý dữ liệu lớn, tốc độ cực nhanh, kết nối liên thông các lĩnh vực kỹ

thuật và phi kỹ thuật, thêm vào nữa là ứng dụng tự động hoá trong sản xuất và đời sống, chẳng hạn robot, xe không người lái....

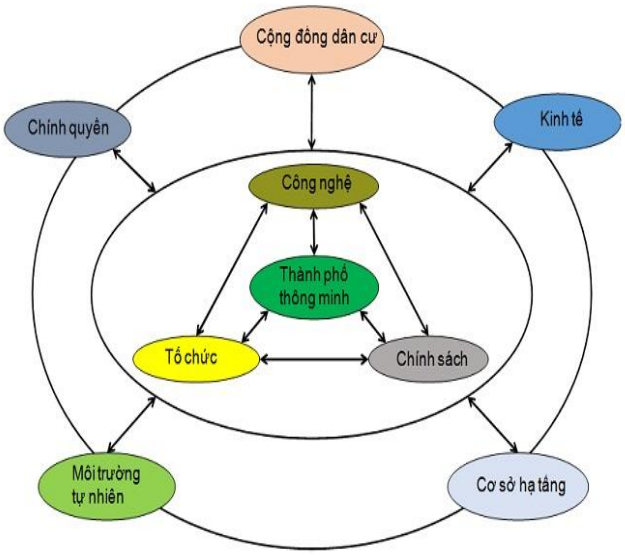
Thứ hai là phải quy hoạch xây dựng một hạ tầng hiện đại, đồng bộ ở những lĩnh vực định ứng dụng các "thông minh" như như giao thông, bệnh viện, trường học... Các lĩnh vực này phải được quy hoạch trong hệ thống nền móng quản lý đô thị bài bản.

Thứ ba là là công dân thông minh (Smart Citizen). Đối tượng chính thực hiện khai thác, sử dụng các hệ thống ứng dụng, dịch vụ cung cấp bởi . Đây được coi là một trong số các yếu tố quyết định sự thành bại của Smart City.

Thứ tư là cần phải có một đội ngũ chuyên gia cực giỏi, toàn diện và trung thành với lợi ích nhân dân để quản lý, vận hành một hệ thống kỹ thuật của Smart City.

Thứ năm là cần phải có "Chính quyền thông minh". Chính quyền thông minh được điều hành bởi các Lãnh đạo thông minh - những người được hỗ trợ bởi hệ thống Chính quyền điện tử, giúp các nhà lãnh đạo ra chính sách, quyết định để duy trì thành quả lâu dài cho Smart City.

Việc nghiên cứu, lên kế hoạch triển khai Smart city giúp đưa ra tầm nhìn tổng thể, đặt ra mục tiêu dài hạn đến phát triển, nhưng phải gắn chặt với các kế hoạch, đề án, dự án ứng dụng CNTT, xây dựng và phát triển chính quyền điện tử, xây dựng các hệ thống thông tin, cơ sở dữ liệu phục vụ chính quyền và người dân. Trong đó, xây dựng, phát triển Chính phủ điện tử sẽ là một trong các yếu tố nền tảng, yếu tố cốt lõi để giúp tạo nên nhân tố chính quyền thông minh hơn, là một nội dung cốt lõi trong xây dựng Smart City.



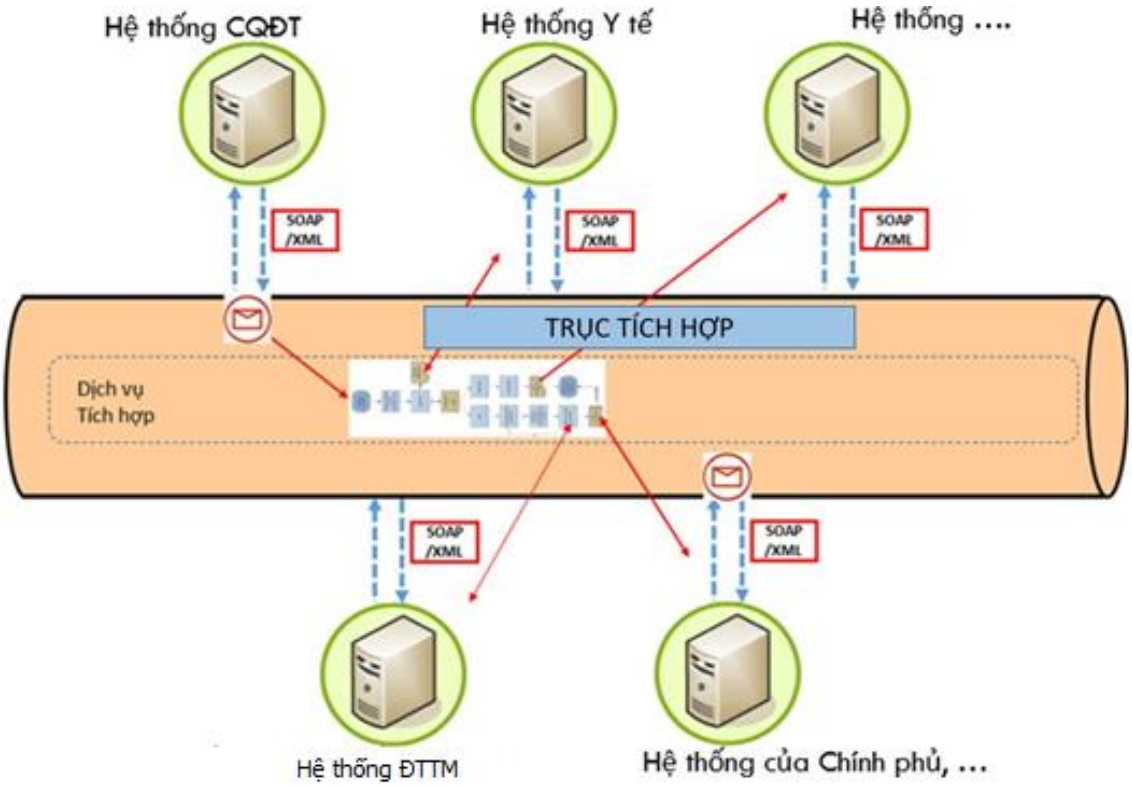
Về cơ bản, chính quyền được định nghĩa "là định chế của luật pháp, quy định hành chính, luật định về hành pháp, tư pháp mà nó ràng buộc các hoạt động của chính quyền trong việc phân phối và hỗ trợ các dịch vụ công cộng". Để thực hiện giám sát việc trao đổi thông tin đúng luật và đạt được mục tiêu đề ra, các tỉnh cần thực hiện triển khai dự án chính quyền điện tử và đây là một trong những yếu tố quan trọng làm nên sự thành công hay thất bại của các dự án xây dựng smart city. Tuy nhiên, khi triển khai chính quyền điện tử sẽ gặp những thách thức về "Mối quan hệ giữa các bên liên quan". Đó chính là khả năng hợp tác giữa các bên, sự hỗ trợ của lãnh đạo, cấu trúc của

liên minh và điều hành dưới phạm vi quyền hạn khác nhau. Việc chuyển đổi từ tỉnh bình thường (không thông minh) sang smart city cũng đòi hỏi sự tương hỗ giữa công nghệ và các thành phần tổ chức chính trị - xã hội trong đó có yếu tố liên quan tới các chính sách về áp dụng ICT, về xây dựng smart city. Trong khi thay đổi công nghệ để xây dựng smart city tương đối dễ dàng, thì việc thay đổi chính sách gặp nhiều khó khăn hơn nên yếu tố chính sách cũng là một trong những thách thức cần phải giải quyết trong quá trình xây dựng một smart city. Ví dụ các tổ chức chính quyền được tạo ra và hoạt động theo các chức năng, nhiệm vụ riêng. Khi triển khai smart city, đưa công nghệ vào ứng dụng sẽ phải thay đổi một lượng lớn các quy định cũ để phù hợp với các quy trình tin học hóa. Việc điều chỉnh sửa đổi này không phải là dễ để có thể áp dụng thống nhất và rộng khắp trong thời gian ngắn.

Có thể nói, việc triển khai xây dựng Smart city phải trên cơ sở tổ chức, xây dựng thành công hệ thống Chính phủ điện tử và các dự án đầu tư ứng dụng Viễn thông - Công nghệ thông tin trong mọi lĩnh vực của tỉnh.

Mô hình triển khai hệ thống Chính quyền điện tử và Đô thị thông minh

Mỗi Đô thị thông minh (ĐTTM) sẽ có nền tảng tích hợp riêng và nền tảng tích hợp của ĐTTM sẽ kết nối với các lĩnh thông minh mà tỉnh muốn ứng dụng trong tương lai (có thể theo thứ tự ưu tiên cho đến khi áp dụng cho toàn bộ các lĩnh vực, khía cạnh đời sống của tỉnh tùy theo mục đích, khả năng tài chính của tỉnh trong tương lai). Hệ thống CPĐT là một trong các lĩnh vực thành phần cốt lõi của ĐTTM và hệ thống CPĐT được tích hợp vào hệ thống hạ tầng CNTT của ĐTTM. Tùy theo điều kiện cụ thể, nền tảng tích hợp LGSP của hệ thống CQĐT hoàn toàn có thể phát triển, nâng cấp, mở rộng thành nền tảng tích hợp của ĐTTM. Một các khái quát, mô hình khái niệm của nền tảng tích hợp của TPTM được trình như hình vẽ sau:



Một số thành phần cơ bản của nền tảng chia sẻ, tích hợp sẽ bao gồm:

- Cổng vào dịch vụ: Cổng vào dịch vụ là giao diện giữa hệ thống ứng dụng của các lĩnh vực nghiệp vụ và nền tảng tích hợp. Khi hệ thống ứng dụng nhận được yêu cầu từ đối tượng (ứng dụng) và muốn kết nối với nền tảng tích hợp, cổng vào dịch vụ sẽ gửi yêu cầu đến để xử lý. Cổng vào dịch vụ cung cấp dịch vụ kiểm soát an ninh, xác nhận định dạng dữ liệu, chuyển đổi định dạng dữ liệu và phân phối tin nhắn.

- Dịch vụ thư mục dùng chung toàn tinh: Dịch vụ thư mục cung cấp cho người dùng một phương thức truy vấn đơn giản mà người dùng có thể sử dụng từ khóa như tên, mã để tìm kiếm thông tin lưu trong máy chủ thư mục. Ví dụ, để đạt được mục tiêu tích hợp mật khẩu, tài khoản, các cơ quan nhà nước có thể sử dụng dịch vụ thư mục để xây dựng tài khoản cho nhân viên đến định danh tài khoản/mật khẩu khác nhau trong các hệ thống khác nhau (cổng thông tin điện tử, thư điện tử, đăng nhập một lần…). Dịch vụ thư mục có thể cung cấp một cơ chế thuận tiện hơn cho người sử dụng và người quản trị để quản lý tài khoản của họ.

- Dịch vụ đăng ký, xác thực: Cung cấp dịch vụ cho đăng ký cung cấp thông tin, đăng ký định vị dịch vụ, đăng ký đối tượng, đăng ký chỉ dẫn mở, luồng dịch vụ đóng gói,… xác thực là quá trình để xác nhận sự thật của các vật thể. Trong hệ thống ĐTTM, đăng ký, xác thực chủ yếu cho các hệ thống ứng dụng. Xác thực hệ thống là quá trình để xác định các hệ thống khác có thể sử dụng nguồn lực của hệ thống. Hầu hết các trường hợp, chứng thư của máy chủ sẽ được sinh ra và có giá trị xác thực máy chủ đó. Khi hệ thống cần phải xác thực một hệ thống khác, có thể định hướng lại quá trình để dịch vụ xác thực dùng chung và dịch vụ chia sẻ sẽ gửi kết quả đến hệ thống ĐTTM để hoàn tất quá trình xác thực máy chủ.

- Dịch vụ quản lý định danh dùng chung: Dịch vụ này cung cấp một cơ chế cho phép các hệ thống chính quyền điện tử nhận dạng người sử dụng. Một số cơ chế có thể được áp dụng để đảm bảo định danh xác định, ví dụ: định danh/mật khẩu cộng với mã xác nhận, hạ tầng khóa công khai, sinh trắc học…Bất kỳ cơ chế định danh nào được sử dụng, việc định danh sẽ tuân thủ theo thủ tục tương tự và do đó, những cơ chế này có thể được xây dựng thành các dịch vụ dùng chung. Khi hệ thống chính quyền điện tử cần định danh ngọời sử dụng, nó có thể sử dụng dịch vụ dùng chung này để hoàn thành việc xác định người sử dụng

- Dịch vụ quản lý nội dung dùng chung: Quản lý nội dung bao gồm quản lý nội dung nền tảng điều hành và các hệ thống ứng dụng phổ biến; quản lý tương tác giữa các nội dung mà không được định nghĩa trong quản lý khác.

- Hạ tầng trao đổi thông tin: Hạ tầng trao đổi thông tin là giao diện giữa Nền tảng tích hợp của Smart City và các nền tảng, hệ thống khác, cho phép cung cấp môi trường phục vụ trao đổi thông tin nghiệp vụ và giao diệncổng thông tin điện tử để hỗ trợ truy xuất và sử dụng dịch vụ thuận tiện. Nó cung cấp cơ chế chuyển đổi và kiểm tra đối với các định dạng thông điệp bên ngoài.

- Dịch vụ nền tảng tích hợp của Smart City: Dịch vụ này nhằm điều phối các ứng dụng hay các dịch vụ để cung cấp các loại dịch vụ mới. Với việc tích hợp, việc đăng ký và tiếp nhận dịch vụ là cần thiết cùng với dịch vụ thư mục, xác thực/cấp quyền và quản lý tài khoản.

- Dịch vụ xác thực và cấp quyền truy cập tập trung: Khi hệ thống hoàn thành quá trình xác

thực, nó sẽ căn cứ vào mức độ quyền hạn khác nhau của hệ thống đã đăng ký, định hướng lại quá trình dịch vụ cấp quyền và các dịch vụ dùng chung sẽ gửi kết quả đến hệ thống để hoàn tất quá trình cấp truyền truy cập.

Giải pháp đề xuất là khi xây dựng ĐTTM, cần lựa chọn cùng một nền tảng công nghệ ESB thống nhất cho cả hệ thống CQĐT và ĐTTM hoặc mở rộng hệ thống Trục liên thông ESB trên nền tảng tích hợp LGSP của hệ thống CQĐT để hình thành Trục liên thông ESB dùng chung toàn tỉnh Bình Phước./.