Gestión de Centro de Cómputos

Prof. Cristian Cabanellas

Prof. Fabio López Pires

Clase 11, 30-03-15

Facultad Politécnica, Universidad Nacional de Asunción

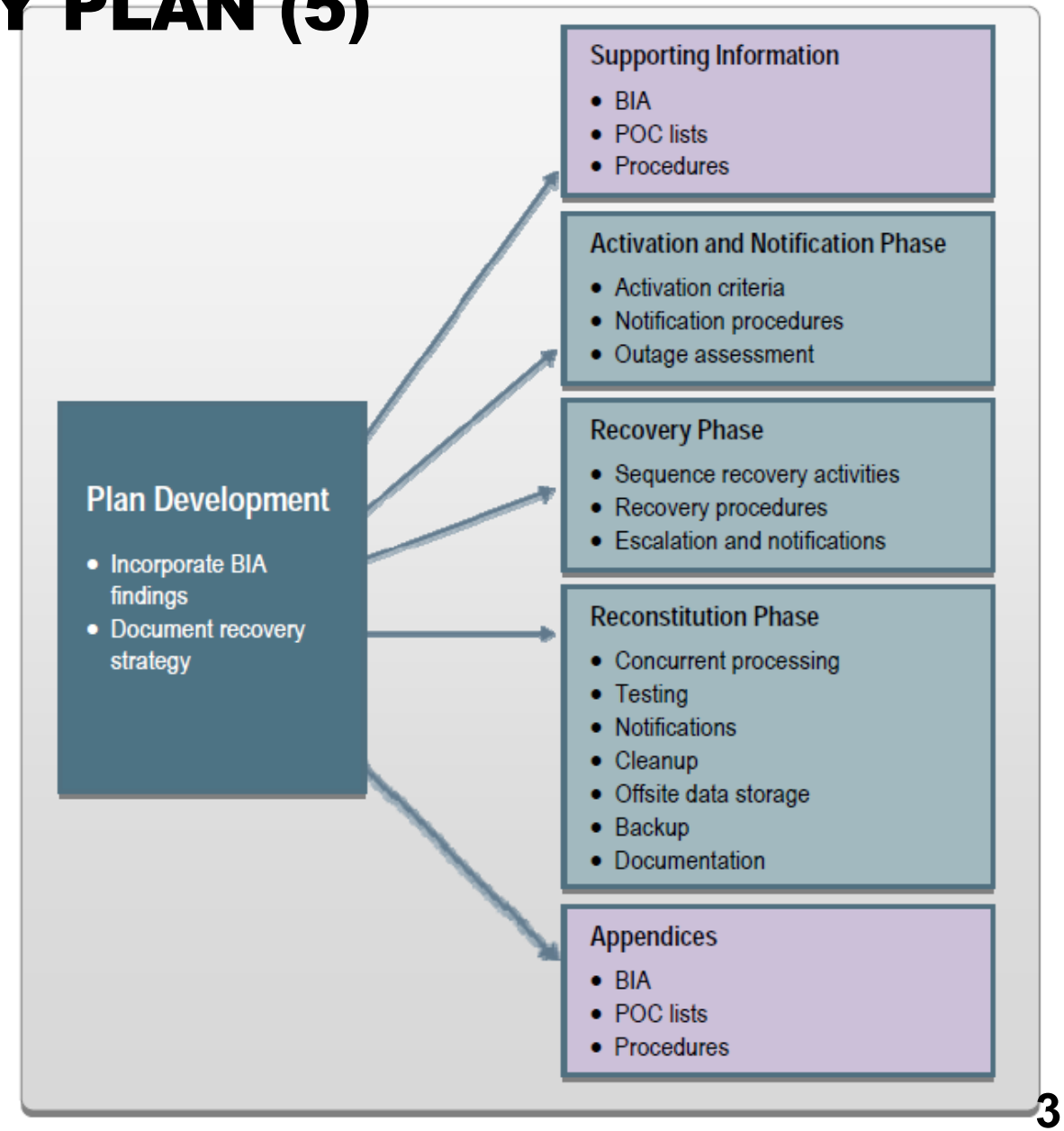
AGENDA

Information System Contingency Planning Process

1. Develop the contingency planning policy;
2. Conduct the business impact analysis (BIA);
3. Identify preventive controls;
4. Create contingency strategies;
5. Develop an information system contingency plan;
6. Ensure plan testing, training, and exercises; and
7. Ensure plan maintenance.

DEVELOP AN INFORMATION SYSTEM CONTINGENCY PLAN (5)

Five main components of the contingency plan



SUPPORTING INFORMATION

The supporting information component includes:

- **Introduction section**
- **concept of operations section**

SUPPORTING INFORMATION

Introduction section

- **Background:** Establishes the reason for developing the ISCP and defines the plan objectives.
- **Scope:** Identifies the FIPS 199 impact level and associated RTOs as well as the alternate site and data storage capabilities (as applicable).
- **Assumptions:** Includes the list of assumptions that were used in developing the ISCP as well as a list of situations that are not applicable.

SUPPORTING INFORMATION

The concept of operations section

- **System description:** Should include the information system architecture, location(s), and any other important technical considerations. An input/output (I/O) diagram and system architecture diagram, including security devices (e.g., firewalls, internal and external connections) are useful.
- **Overview of three phases:** The ISCP recovery is implemented in three phases: (1) Activation and Notification, (2) Recovery, and (3) Reconstitution.
- **Roles and responsibilities:** Presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. Also provides an overview of team member roles and responsibilities in a contingency situation.

ACTIVATION AND NOTIFICATION PHASE

Defines initial actions taken once a system disruption or outage has been detected or appears to be imminent.

This phase includes:

- **activities to notify recovery personnel,**
- **conduct an outage assessment, and**
- **activate the plan.**

At the completion of the Activation and Notification Phase, ISCP staff will be prepared to perform recovery measures to restore system functions.

ACTIVATION AND NOTIFICATION PHASE

Activation criteria may be based on:

- **Extent of any damage to the system (e.g., physical, operational, or cost);**
- **Criticality of the system to the organization's mission (e.g., critical infrastructure protection asset); and**
- **Expected duration of the outage lasting longer than the RTO.**

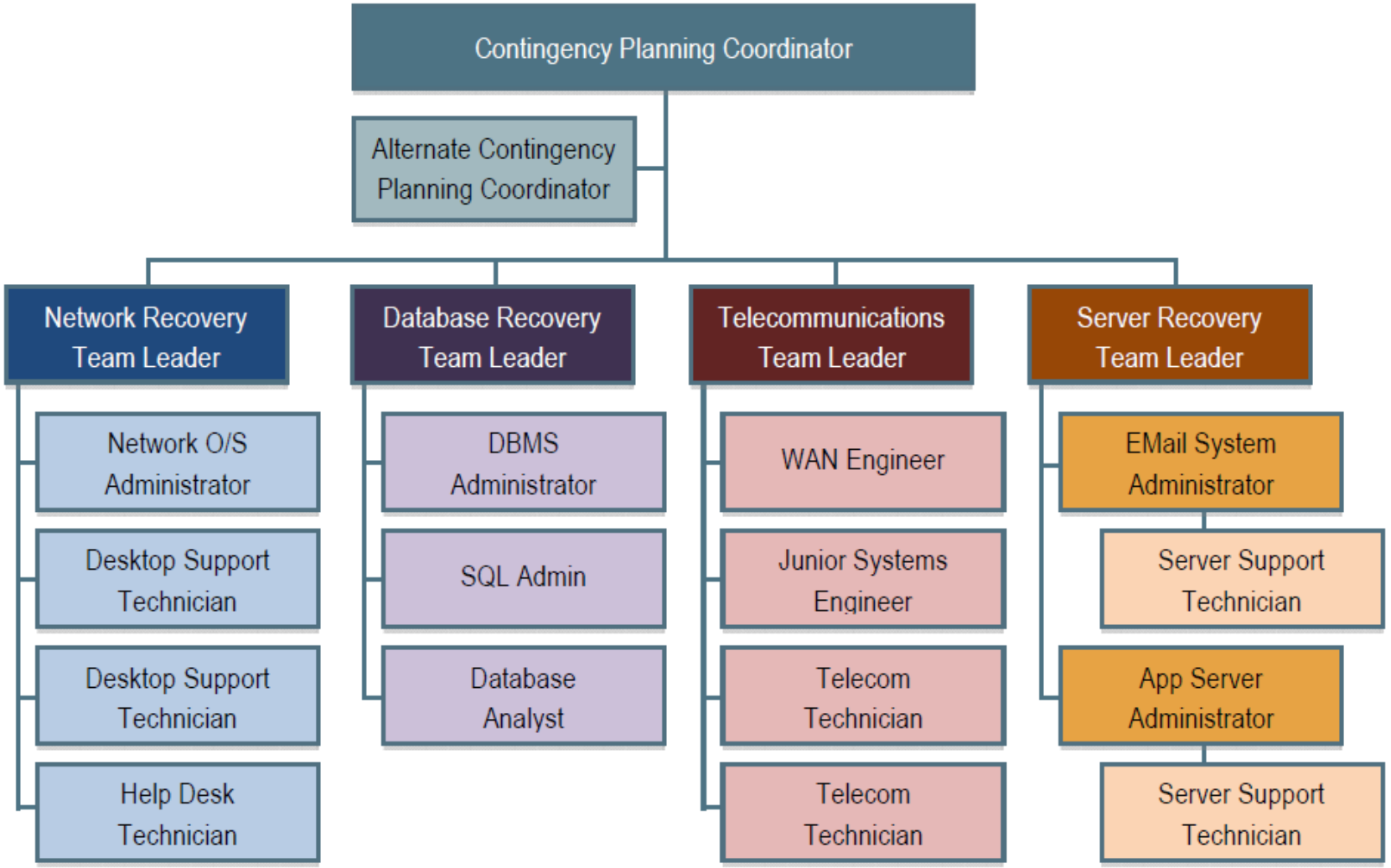
ACTIVATION AND NOTIFICATION PHASE

Notification Procedures:

The procedures should describe the methods used to notify recovery personnel during business and non business hours.

Prompt notification is important for reducing the effects of a disruption on the system; in some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash.

ACTIVATION AND NOTIFICATION PHASE: CALL TREE



ACTIVATION AND NOTIFICATION PHASE

Call Tree format:

- **Systems Software Team**
- **Team Leader—Primary**
- **Jane Jones**
- **1234 Any Street**
- **Town, State, Zip Code**
- **Home: (123) 456-7890**
- **Work: (123) 567-8901**
- **Cell: (123) 678-9012**
- **Email: jones@organization.ext; jones@home.ext**

ACTIVATION AND NOTIFICATION PHASE

Outage assessment procedures may be unique for the particular system, but the following minimum areas should be addressed:

- **Cause of the outage or disruption;**
- **Potential for additional disruptions or damage;**
- **Status of physical infrastructure (e.g., structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation and air-conditioning [HVAC]);**
- **Inventory and functional status of system equipment (e.g., fully functional, partially functional, nonfunctional);**
- **Type of damage to system equipment or data (e.g., water, fire and heat, physical impact, electrical surge);**
- **Items to be replaced (e.g., hardware, software, firmware, supporting materials); and**
- **Estimated time to restore normal services.**

RECOVERY PHASE

Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location. At the completion of the Recovery Phase, the information system will be functional and capable of performing the functions identified in the plan.

RECOVERY PHASE

1. Sequence of Recovery Activities
2. Recovery Procedures
3. Recovery Escalation and Notification

RECOVERY PROCESS

SAMPLE Recovery Process for the LAN Recovery Team:

- **These procedures are used for recovering a file from backup tapes. The LAN Recovery**
- **Team is responsible for reloading all critical files necessary to continue production.**

1. **Identify file and date from which file is to be recovered.**
2. **Identify tape number using tape log book.**
3. **If tape is not in tape library, request tape from recovery facility; fill out with appropriate authorizing signature.**
4. **When tape is received, log date and time.**
5. **Place tape into drive and begin recovery process.**

RECONSTITUTION PHASE

The Reconstitution Phase is the third and final phase of ISCP implementation and defines the actions taken to test and validate system capability and functionality. During Reconstitution, recovery activities are completed and normal system operations are resumed.

This phase consists of two major activities:

- validating successful recovery
- deactivation of the plan

RECONSTITUTION PHASE

Validation of recovery typically includes these steps:

- **Concurrent Processing: Is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.**
- **Validation Data Testing: Is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.**
- **Validation Functionality Testing: Is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.**

RECONSTITUTION PHASE

Deactivation of the plan activities include:

- **Notifications: Upon return to normal operations, users should be notified by the ISCP Coordinator (or designee) using predefined notification procedures.**
- **Cleanup: Is the process of cleaning up work space or dismantling any temporary recovery locations, restocking supplies, returning manuals or other documentation to their original locations, and readying the system for another contingency event.**

RECONSTITUTION PHASE

- **Offsite Data Storage: If offsite data storage is used, procedures should be documented for returning retrieved backup or installation media to its offsite data storage location.**
- **Data Backup: As soon as reasonable following reconstitution, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup should be stored with other system backups and comply with applicable security controls.**
- **Event Documentation: All recovery and reconstitution events should be well documented, including actions taken and problems encountered during the recovery and reconstitution efforts. An after-action report with lessons learned should be documented and included for updating the ISCP.**

PLAN APPENDICES

Contingency plan appendices provide key details not contained in the main body of the plan. Common contingency plan appendices include the following:

- **Contact information for contingency planning team personnel;**
- **Vendor contact information, including offsite storage and alternate site POCs; BIA;**
- **Detailed recovery procedures and checklists;**
- **Detailed validation testing procedures and checklists;**
- **Equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations. Details should be provided for each entry, including model or version number, specifications, and quantity;**
- **Alternate mission/business processing procedures that may occur while recovery efforts are being done to the system;**
- **ISCP testing and maintenance procedures;**
- **System interconnections (systems that directly interconnect or exchange information); and**
- **Vendor SLAs, reciprocal agreements with other organizations, and other vital records.**

AGENDA

Information System Contingency Planning Process

1. Develop the contingency planning policy;
2. Conduct the business impact analysis (BIA);
3. Identify preventive controls;
4. Create contingency strategies;
5. Develop an information system contingency plan;
6. Ensure plan testing, training, and exercises; and
7. Ensure plan maintenance.

ENSURE PLAN TESTING, TRAINING, AND EXERCISES (6)

An ISCP should be maintained in a state of readiness, which includes having personnel trained to fulfill their roles and responsibilities within the plan, having plans exercised to validate their content, and having systems and system components tested to ensure their operability in the environment specified in the ISCP

ENSURE PLAN TESTING, TRAINING, AND EXERCISES (6)

Organizations should conduct TT&E events periodically, following organizational or system changes, or the issuance of new TT&E guidance, or as otherwise needed. Execution of TT&E events assists organizations in determining the plan's effectiveness, and that all personnel know what their roles are in the conduct of each information system plan.

ENSURE PLAN TESTING, TRAINING, AND EXERCISES (6)

Testing:

- **Tests are evaluation tools that use quantifiable metrics to validate the operability of an information system or system component in an operational environment. For example, an organization could test call tree lists to determine if calling can be executed within prescribed time limits.**
- **A test is conducted in as close to an operational environment as possible.**
- **The scope of testing can range from individual system components or systems to comprehensive tests of all systems and components that support an ISCP.**
- **Tests often focus on recovery and backup operations.**

ENSURE PLAN TESTING, TRAINING, AND EXERCISES (6)

Testing, the following areas should be addressed in a contingency plan test, as applicable:

- **Notification procedures;**
- **System recovery on an alternate platform from backup media;**
- **Internal and external connectivity;**
- **System performance using alternate equipment;**
- **Restoration of normal operations; and**
- **Other plan testing (where coordination is identified, i.e., COOP, BCP).**

ENSURE PLAN TESTING, TRAINING, AND EXERCISES (6)

Training:

- **Training refers only to informing personnel of their roles and responsibilities within a particular information system plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to the ISCP.**
- **Training personnel on their roles and responsibilities before an exercise or test event is typically split between a presentation on their roles and responsibilities and activities that allow personnel to demonstrate their understanding of the subject matter.**

ENSURE PLAN TESTING, TRAINING, AND EXERCISES (6)

Recovery personnel should be trained on the following plan elements:

- **Purpose of the plan;**
- **Cross-team coordination and communication;**
- **Reporting procedures;**
- **Security requirements;**
- **Team-specific processes (Activation and Notification, Recovery, and Reconstitution Phases); and**
- **Individual responsibilities (Activation and Notification, Recovery, and Reconstitution Phases).**

ENSURE PLAN TESTING, TRAINING, AND EXERCISES (6)

Exercises:

- **An exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an ISCP. In an exercise, personnel with roles and responsibilities in a particular ISCP meet to validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment.**
- **Exercises are scenario-driven, such as a power failure in one of the organization's data centers or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise.**

ENSURE PLAN TESTING, TRAINING, AND EXERCISES (6)

The following types of exercises widely used in information system TT&E programs by single organizations:

- **Tabletop Exercises: Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.**

ENSURE PLAN TESTING, TRAINING, AND EXERCISES (6)

- **Functional Exercises: Allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.**

ISCP TT&E ACTIVITIES

TT&E Event	Sample Activity	FIPS 199 Availability Security Objective
ISCP Training (CP-3)	A seminar and/or briefing used to familiarize personnel with the overall ISCP purpose, phases, activities, and roles and responsibilities.	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Instruction (CP-3)	Instruction of contingency personnel on their roles and responsibilities within the ISCP and includes refresher training. (For a high-impact system, incorporate simulated events.)	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Contingency Plan Test / Exercise (CP-4)	Test and/or exercise the contingency plan to determine effectiveness and the organization's readiness. This could include planned and unplanned maintenance activities	Low Impact = Yes Mod. Impact = Yes High Impact = Yes
Tabletop Exercise (CP-4)	Discussion-based simulation of an emergency situation in an informal, stress-free environment; designed to elicit constructive scenario-based discussions for an examination of the existing ISCP and individual state of preparedness.	Low Impact = Yes

ISCP TT&E ACTIVITIES

TT&E Event	Sample Activity	FIPS 199 Availability Security Objective
Functional Exercise (CP-4)	Simulation of a disruption with a system recovery component such as backup tape restoration or server recovery.	Mod. Impact = Yes High Impact = Yes
Full-Scale Functional Exercise (CP-4)	Simulation prompting a full recovery and reconstitution of the information system to a known state and ensures that staff are familiar with the alternate facility.	High Impact = Yes
Alternate Processing Site Recovery (CP-4, CP-7)	Test/exercise the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and evaluate the site's capabilities to support contingency operations. Includes a full recovery and return to normal operations to a known secure state. *(*For a high-impact system, the alternate site should be fully configured as defined in the plan.*)*	Low Impact = N/A Mod. Impact = N/A High Impact = Yes
System Backup (CP-9)	Test backup information to verify media reliability and information integrity. (For a high-impact system, use sample backup information and ensure that backup copies are stored in a separate facility.)	Low Impact = N/A Mod. Impact = Yes High Impact = Yes

AGENDA

Information System Contingency Planning Process

1. Develop the contingency planning policy;
2. Conduct the business impact analysis (BIA);
3. Identify preventive controls;
4. Create contingency strategies;
5. Develop an information system contingency plan;
6. Ensure plan testing, training, and exercises; and
7. Ensure plan maintenance.

ENSURE PLAN MAINTENANCE (7)

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies.

As a general rule, the plan should be reviewed for accuracy and completeness at an organization-defined frequency or whenever significant changes occur to any element of the plan. Certain elements, such as contact lists, will require more frequent reviews. The plans for moderate- or high-impact systems should be reviewed more often.

ENSURE PLAN MAINTENANCE (7)

At a minimum, plan reviews should focus on the following elements:

- **Operational requirements;**
- **Security requirements;**
- **Technical procedures;**
- **Hardware, software, and other equipment (types, specifications, and amount);**
- **Names and contact information of team members;**
- **Names and contact information of vendors, including alternate and offsite vendor POCs;**
- **Alternate and offsite facility requirements; and**
- **Vital records (electronic and hardcopy).**

FUENTES Y LECTURAS ADICIONALES

- **Contingency Planning Guide for Federal Information Systems, NIST Special Publication 800-34 Rev. 1.**

THE END