DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES
KAGAWARAN NG KAPALIGIRAN AT LIKAS YAMAN

BAGONG PILIPINAS

MEMORANDUM

TO : **All Regional Offices**
All Bureaus
All Attached Agencies

THRU : **The Director**
Knowledge and Information Systems Service

FROM : **The Undersecretary**
Finance, Information Systems and Climate Change

SUBJECT : **CYBERSECURITY CAMPAIGN PROGRAM REPORT**

DATE : JAN 0 3 2024

This is to furnish you with a copy of the reports on the Cybersecurity Campaign Program:

I. **Awareness Seminar (October 9-10, 2023)**

The cybersecurity awareness program kicked off with a ribbon-cutting ceremony at the Department of Environment and Natural Resources (DENR) Central Office, led by Secretary Maria Antonia Yulo Loyzaga, Undersecretary Analiza Rebuelta-Teh, and other officials. The program aimed to raise awareness and educate DENR employees and officials on cybersecurity through a seminar and exhibits from IT partners. The seminar covered various topics, including the National Cybersecurity Plan 2023-2028, data privacy and security, cybersecurity bureau operations and services, cybersecurity threats landscape, digital parenting, practical tips to avoid online scams and cybercrimes, balancing convenience and security, and the human firewall. Speakers from various organizations, such as the Department of Information and Communications Technology (DICT), National Privacy Commission, Philippine National Computer Emergency Response Team (NCERT/CERT-PH), Digital Certificate Division, Critical Infrastructure Evaluation and Cybersecurity Standards Monitoring Division, Cybercrime Investigation and Coordinating Center (CICC), Trend Micro, WhosCall, WiSAP, and ePLDT provided insights and expertise on their respective topics. The program concluded with the awarding of certificates, photo ops, and closing remarks by Director Arlene A. Romasanta.

II. **Technical Training (October 18-21, 2023)**

The technical training portion of the cybersecurity campaign program conducted on October 18-21, 2023, was introduced by Christine Apple B. Pre from the Department of Information and Communications Technology (DICT). The speakers include Mr. Alwell C. Mulsid, Mr. Ned G. Serate, and Mr. Zairo Shin F. Maniacop. Mr. Mulsid discussed cyber threat landscapes, incident response, and preparation and prevention measures. Mr. Serate covered vulnerability management and ethical hacking, while Mr. Maniacop focused on incident handling and management. The participants completed a post-assessment and participated in a

MEMO NO. 2024 - 03

group activity called "Cybersecurity Tabletop Exercise." The activity involved solving six scenarios related to cybersecurity incidents and sharing solutions with other groups. The training concluded with the awarding of certificates to all speakers and closing remarks by Eugene C. De Guzman from KISS-NIMD.

For your information.

ATTY. ANALIZA REBUELTA-TEH

DEPARTMENT OF ENVIRONMENT AND NATURAL RESOURCES
KAGAWARAN NG KAPALIGIRAN AT LIKAS YAMAN

BAGONG PILIPINAS

MEMORANDUM

FOR : **The Undersecretary**
Finance, Information Systems and Climate Change

FROM : **The Director**
Knowledge and Information Systems Service

SUBJECT : **SUBMISSION OF CYBERSECURITY CAMPAIGN PROGRAM REPORT**

DATE : 12 DEC 2023

We respectfully submit the following report as part of the Cybersecurity Campaign Program:

I. Awareness Seminar (October 9-10, 2023)

The cybersecurity awareness program kicked off with a ribbon cutting ceremony at the Department of Environment and Natural Resources (DENR) Central Office, led by Secretary Maria Antonia Yulo Loyzaga, Undersecretary Analiza Rebuelta-Teh and other officials. The program aimed to raise awareness and educate DENR employees and officials on cybersecurity through a seminar and exhibits from IT partners. The seminar covered various topics, including the National Cybersecurity Plan 2023-2028, data privacy and security, cybersecurity bureau operations and services, cybersecurity threats landscape, digital parenting, practical tips to avoid online scams and cybercrimes, balancing convenience and security, and the human firewall. Speakers from various organizations, such as the Department of Information and Communications Technology (DICT), National Privacy Commission, Philippine National Computer Emergency Response Team (NCERT/CERT-PH), Digital Certificate Division, Critical Infrastructure Evaluation and Cybersecurity Standards Monitoring Division, Cybercrime Investigation and Coordinating Center (CICC), Trend Micro, WhosCall, WiSAP, and ePLDT provided insights and expertise on their respective topics. The program concluded with the awarding of certificates, photo ops, and closing remarks by Director Arlene A. Romasanta.

II. Technical Training (October 18-21, 2023)

The technical training portion of the cybersecurity campaign program conducted on October 18-21, 2023, was introduced by Christine Apple B. Pre from the Department of Information and Communications Technology (DICT). The speakers include Mr. Alwell C. Mulsid, Mr. Ned G. Serate, and Mr. Zairo Shin F. Maniacop. Mr. Mulsid who discussed cyber threat landscapes, incident response, and preparation and prevention measures. Mr.

Serate covered vulnerability management and ethical hacking, while Mr. Maniacop focused on incident handling and management.

The participants completed a post assessment and participated in a group activity called "Cybersecurity Tabletop Exercise." The activity involved solving six scenarios related to cybersecurity incidents and sharing solutions with other groups. The training concluded with the awarding of certificates to all speakers and closing remarks by Eugene C. De Guzman from KISS-NIMD.

For your information.

ARomasanta
ARLENE A. ROMASANTA

CYBERSECURITY CAMPAIGN PROGRAM

October 9-10, 2023
Department of Environment and Natural Resources - Central Office
2nd Flr Social Hall, Quezon City

I. Awareness Seminar

A. Introduction

Cybersecurity awareness training is the process of educating people or employees to understand, identify, and avoid cyber threats. The ultimate goal is to prevent or mitigate harm to both the Department and its stakeholders and reduce human cyber risk. The training programs will ensure businesses, employees as well as outside contractors, and business partners will follow processes that protect the computer system of an organization from a data breach.

Research suggests that human error is involved in more than 90% of security breaches. Security awareness training helps to minimize risk thus preventing the loss of Personal Identifiable Information (PII), Intellectual Property (IP), money or brand reputation. An effective awareness training program addresses the cybersecurity mistakes that employees may make when using email, the web and in the physical world such as tailgating or improper document disposal.

Today, any lapse in cyber security can have real repercussions for organizations. One simple error can lead to serious damage for both the individual and the company, who must report the incident to regulators as well as their customers. The cost of a security breach has never been higher, and client or customer are increasingly willing to walk away from businesses and platforms that can not protect their data. As a result, the risk for many companies is too great to ignore.

Cybersecurity awareness is a journey - by regularly providing cybersecurity awareness training to employees in a fun and educating way, you can make cybersecurity everyone's role.

B. Objectives

The seminar aims to:

1. Enhance organizational resilience against cyber threats;
2. Create a shift in employee mindset and behavior change towards information security;
3. Generate buy-in and commitment towards cyber security initiatives;
4. Improve audit results and demonstrate regulatory compliance; and
5. Reduce human error and mitigate security risks.

C. Participants

A total of one hundred three (103) participants, seventy six (76) attended the face-to-face seminar and twenty seven (27) attended thru online.

C. Event & Program

The cybersecurity awareness program started with a ribbon cutting at the lobby of Department of Environment and Natural Resources - Central Office led by Secretary Maria Antonia Yulo Loyzaga together with Undersecretary Analiza Rebuelta-Teh and Director Arlene A. Romasanta; with the presence of Head Executive Assistant Jose Joaquin Y. Loyzaga, Undersecretary Ernesto D. Adobo Jr., Undersecretary Juan Miguel T. Cuna, Undersecretary Carlos Primo C. David, Assistant Secretary Hiro V. Masuda, Assistant Secretary Michelle Angelica D. Go, Assistant Secretary Daniel Darius M. Nicer, Director Norlito A. Eneran, and Director Rolando R. Castro. This was followed by the Cybersecurity Awareness Seminar at the 2nd floor of DENR-CO Social Hall started with the invocation prayer and a keynote message from Secretary Maria Antonia Yulo-Loyzaga on how cyberattack can occur to any organizations private or government. Secretary also included in her message how the Covid-19 Pandemic shifted the services and transactions online and increased the volume of digital interactions of people that makes them a gateway for possible cyber attacks. Afterwards, Undersecretary Analiza Rebuelta-Teh gave her welcome remarks as she honored guests from the Department of Information and Communications Technology (DICT) and IT partners from different IT companies. Undersecretary Teh incorporates in her message the aim of the seminar which is to raise awareness and educate each employee and officials of DENR to become vigilant guardians of our digital world as threats of cyber attacks, scams, and phishing schemes. In addition, Director Arlene A. Romasanta introduced and invited all participants and employees to visit and explore different booths and exhibits from IT partners at the ground floor lobby of DENR-CO and to immerse themselves in the different advanced technologies and innovations in network security, information security, and disaster recovery and business continuity.

D. Lecture/Discussion (First Day)

TOPICS/DISCUSSION	RESOURCE SPEAKER
National Cybersecurity Plan 2023-2028 ❖ Vision of National Cybersecurity Plan 2023-2028 ❖ Cybersecurity Policy Framework ❖ Enhancing the implementation of existing cybersecurity and cyber crime laws, rules, and regulations ❖ Proposal of new legislative measures to strengthen cybersecurity	**Engr. Carlos P. Reyes** Director, Cybersecurity Bureau
Data Privacy and Security ❖ Personal Information vs Sensitive Personal Information ❖ Data privacy principles ❖ Rights of a data subject ❖ Basis on processing personal information and sensitive personal information ❖ Principles of Information Security ❖ Types of security measures ❖ Cybersecurity and data privacy protection tips ❖ Data breach	**Atty. Amor Venenoso** Attorney III, Compliance and Monitoring Division National Privacy Commission

➢ Types and examples ➢ Team and responsibilities	

After the discussion of each speaker, it was followed by the awarding of the Certificate of Appreciation for imparting their knowledge and expertise on their topics discussed. The activity ended with closing remarks for day one.

E. Lecture/Discussion (Second Day)

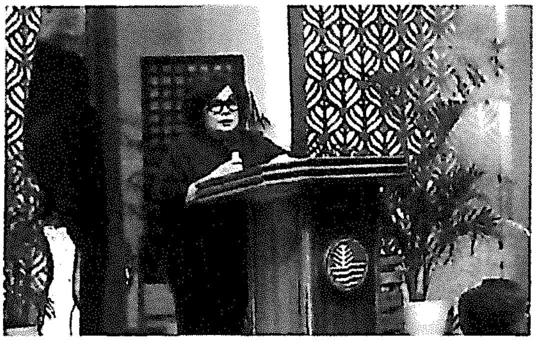
TOPICS/DISCUSSION	RESOURCE SPEAKER
Cybersecurity Bureau Cert-PH Operations and Services and Cybersecurity Threat Landscape ❖ Philippine National Computer Emergency Response Team (NCERT/CERT-PH) ❖ CERT-PH operations and services ❖ National security operations center ❖ Cybersecurity vulnerabilities and recommendations ❖ Safeguarding the CERT environment	**Engr. George P. Tardio** OIC Chief, Critical Infrastructure Evaluation and Cybersecurity Standard Monitoring Division DICT
Philippine National Public Key Infrastructure (PNPKI) ❖ PKI vs PNPKI ❖ Components of PKI ❖ Digital certificates ❖ Digital signatures ❖ Benefits of PNPKI ❖ Legal basis of e-signature and PNPKI ❖ Application and requirements	**Jennifer B. Canlas** Information Technology Officer I Digital Certificate Division DICT
Cyber Hygiene ❖ Kinds of cyber threats ❖ Benefits of cyber hygiene ❖ Cyber hygiene protocols and policies checklist ❖ Cyber hygiene best practices for organizations and individuals	**Christine Apple B. Pre** Information Officer III Critical Infrastructure Evaluation and Cybersecurity Standards Monitoring Division DICT
Digital Parenting ❖ Objective of digital parenting ❖ Challenges of digital parenting ❖ Effects of gadget on kids ❖ Gadget screen time guidelines by age ❖ Steps in good digital parenting ❖ Parental controls ❖ Positive and negative impacts of technology on children ❖ Risk to consider, safety measures to take, and how to prevent attacks when using an online platform	**Maricar G. Magpili** Information Technology Officer I Critical Infrastructure Evaluation and Cybersecurity Standards Monitoring Division DICT

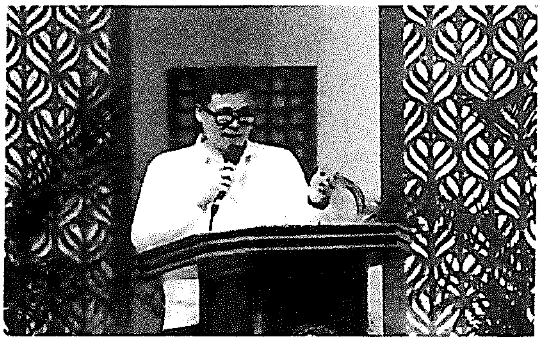
Practical Tips and Scenarios to Avoid Online Scams and Cyber Crimes ❖ Attack Landscape ❖ Cybercrime Investigation and Coordinating Center (CICC) ❖ CICC forms and procedures on tagging, chain of custody and live digital forensics ❖ CICC national cybercrime hub ❖ Women in cyber the offense and defense strategy ❖ CICC home developed platform	**Asec. Mary Rose Magsaysay** Deputy Executive Director Cybercrime Investigation and Coordinating Center (CICC)
CyberHygiene: Protecting your Digital Footprint ❖ Cyber attack target/s ❖ Common type of attack and breaches ❖ Identity protection ❖ Definition and categories of phishing ❖ Common types of malware ❖ Types of email threats	**Rodel Villarez** Principal Technical Educator Trend Micro
Demystifying Fraud ❖ Fraud vs Scam ❖ Fraud landscape ❖ Persona of a fraudster ❖ Usage of AI in fraud ❖ Fraud impact on next generation	**Maria Carmela Migriño** Southeast Asia Regional Director for Information Security and Regulatory Alliance WhosCall
Scam Free Pilipinas Campaign ❖ WhosCall App (scam detection application) ➢ Message and caller ID ➢ URL scanner ➢ Number report ➢ Blocker ➢ Number Search	**Gabriel Roberto Agoncillo Barrios** Country Marketing Head, PH WhosCall
Balancing Convenience and Security: Building a Culture of Security and Privacy ❖ The evolving threat landscape ❖ Threat landscape impact ❖ Layered security and zero trust adoption ❖ Steps on managing cyber incidents ❖ Roles of cyber incidents ❖ Cyber crisis management team ❖ Data protection controls in reference to the Philippine data privacy act ❖ Checklist for the safer hybrid environment	**Maria Carmela Migriño** Chairman and President WiSAP

The Color of Cybersecurity: The Green Team in All of Us ❖ Cybercrime ❖ Malware ❖ Ransomware ❖ Bots ❖ Social Engineering ❖ Cybersecurity color wheel ❖ How can you better protect yourself online ❖ Reality check	**Alvic A. Osorio** Solutions Architect Trends and Technologies, Inc **Alvic A. Osorio** Solutions Architect Trends and Technologies, Inc
The Human Firewall: Your Critical Role in Public Sector Security (Securing the Digital Transformation Journey) ❖ Breaches (National Government Agencies) ➢ Breaches timeline ➢ Cause of breaches ➢ Notable breaches - government agencies ❖ Cybersecurity Statistics ❖ Recorded cyber attacks ❖ Customer breaches ➢ Breached through IoT devices ➢ Breached through vulnerable web app ➢ Breached through malicious email attachment ➢ Breached through compromise corporate account ➢ Breached through zero-day attack ❖ Essential security measure to follow and recommendations ❖ Operationalizing cybersecurity	**Reynaldo J. Suarez Jr.** Business Consultant for Cybersecurity ePLDT

After the discussion of the speakers, it was followed by the awarding of certificates, photo ops and closing remarks led by Director of Knowledge and Information Systems Service, Director Arlene A. Romasanta.

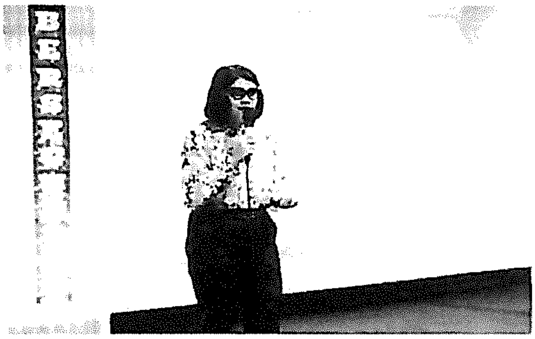
F. Photo Documentation



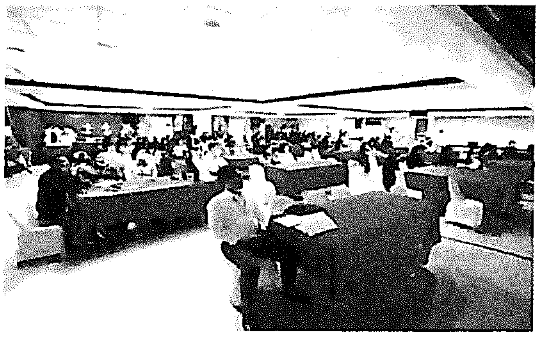


ERSECURIT

RENESS



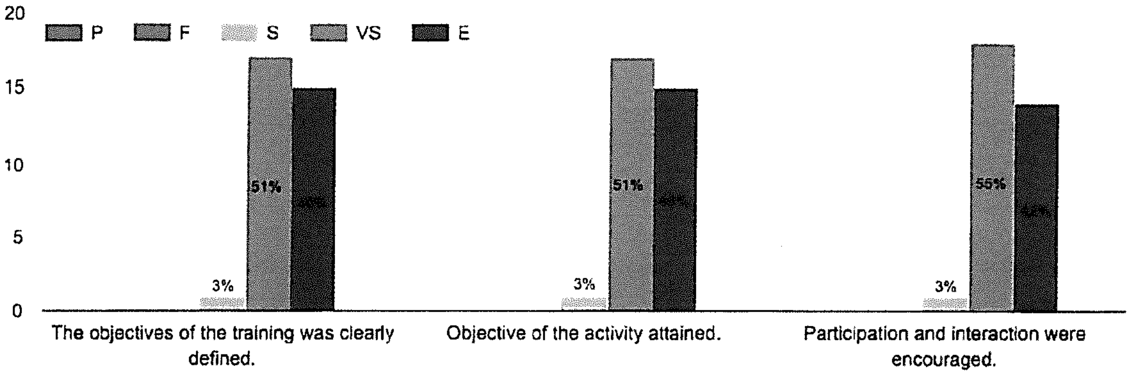
Powered by



G. Evaluation Survey Result for the Awareness Seminar dated October 9 - 10, 2023

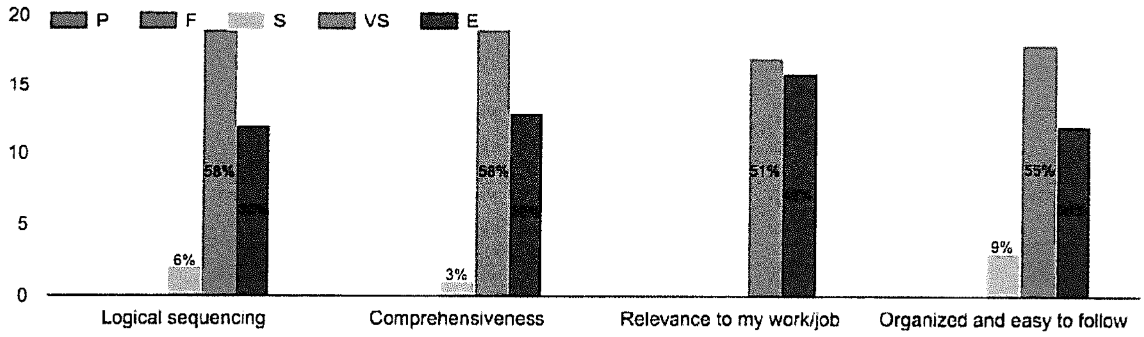
a. Substantive Matters

1.) OBJECTIVE OF THE EVENT



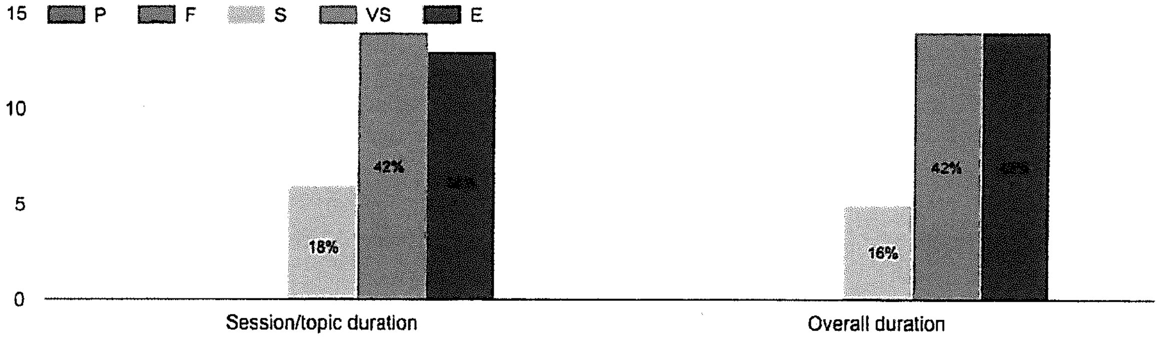
A total of 33 responses for the objective of the event and were categorized in three parts : the objectives of the training was clearly defined, the objective of the activity attained and the participation and interaction were encouraged. First, for the part of "objectives of the training was clearly defined", 46% of the participants voted for excellent, 51% voted for very satisfactory and 3% voted for satisfactory. Second for the part of "objective of the activity attained" 46% of the participants voted for excellent, 51% voted for very satisfactory and 3% voted for satisfactory. Lastly, for the "participation and interaction were encouraged" 42% of the participants voted for excellent, 55% voted for very satisfactory and 3% voted for satisfactory.

2.) TOPICS



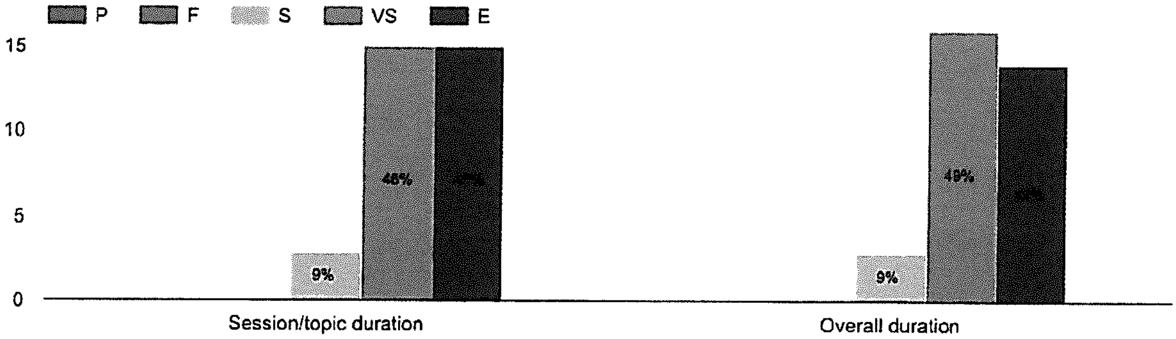
A total of 33 responses for the topics and were categorized in four parts : the logical sequencing, the comprehensiveness, the relevance to my work/job, and the organized and easy to follow. First, for the part of logical sequencing, 36% of the participants voted for excellent, 58% voted for very satisfactory, 6% voted for satisfactory. Second, for the comprehensiveness 39% of the participants voted for excellent, 58% voted for very satisfactory and 3% voted for satisfactory. Third, for the "relevance to my work/job", 49% of the participants voted for excellent and 51% voted for very satisfactory. Lastly, for the "organized and easy to follow" 55% of the participants voted for excellent, 36% voted for very satisfactory and 9% voted for satisfactory.

3.) TIME AND SCHEDULE



A total of 33 responses for the time and schedule and were categorized in two parts : the session/topic duration and the overall duration. For the "session/topic duration" 40% of the participants voted for excellent, 42% voted for very satisfactory and 18% voted for satisfactory. The "overall duration" 42% percent of the participants voted for excellent, 42% voted for satisfactory and 16% voted for satisfactory.

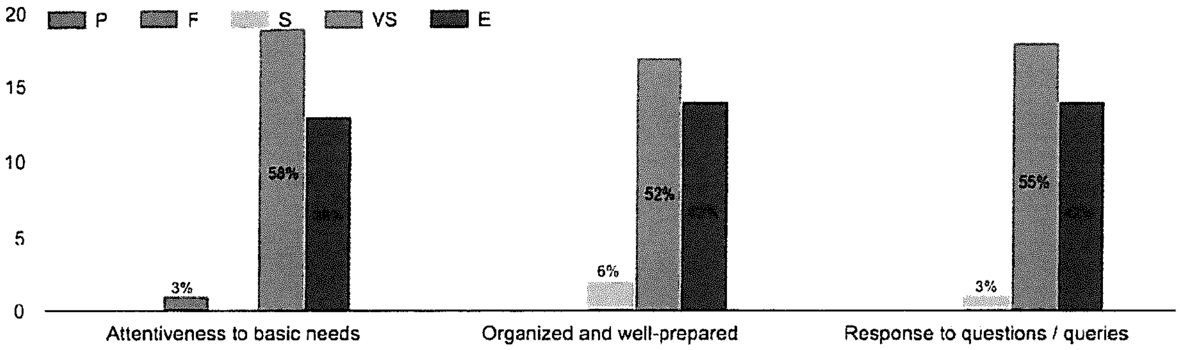
4.) METHODOLOGY



A total of 33 responses for the methodology and were categorized in two parts : the session/topic duration and the overall duration. For the "session/topic duration" 45% of the participants voted for excellent, 46% voted for very satisfactory and 9% voted for satisfactory. On the "overall duration" 42% of the participants voted for excellent, 49% voted for very satisfactory and 9% voted for satisfactory.

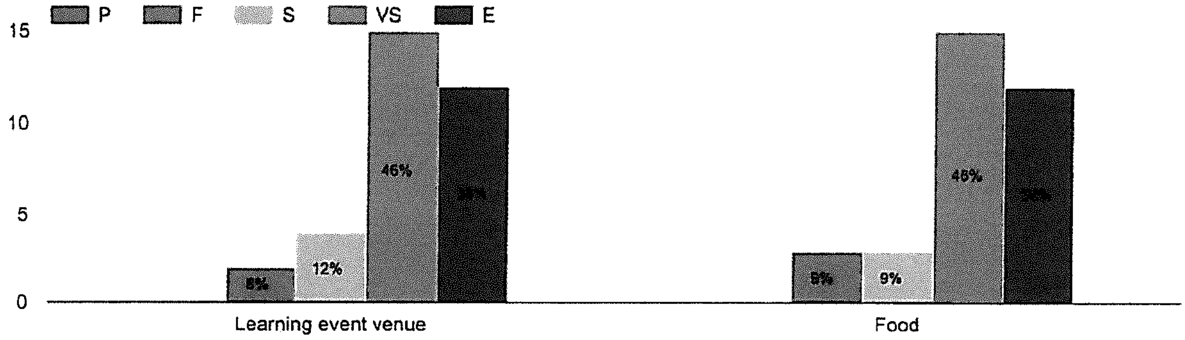
b. Administrative Matters

1.) Learning Event Team



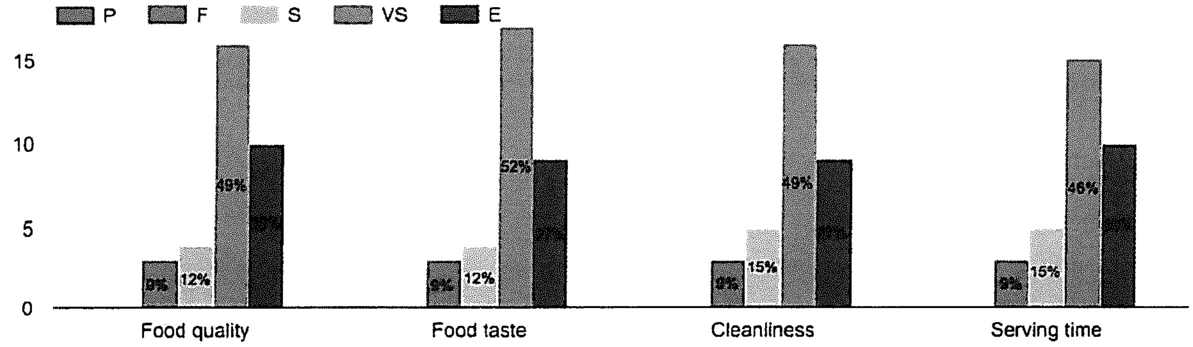
A total of 33 responses for the learning event team and were categorized in three parts : the attentiveness to basic need, the organized and well-prepared and the response to questions/queries. First, for the "attentiveness to basics needs" 39% of the participants voted for excellent, 58% voted for very satisfactory and 3% voted for fair. Second, for the "organized and well prepared" 42% of the participants voted for excellent, 52% voted for very satisfactory and 6% voted for satisfactory. Lastly, for the "response to questions/queries" 42% of the participants voted for excellent, 55% voted for very satisfactory and 3% voted for satisfactory.

2.) Accommodation and Venue



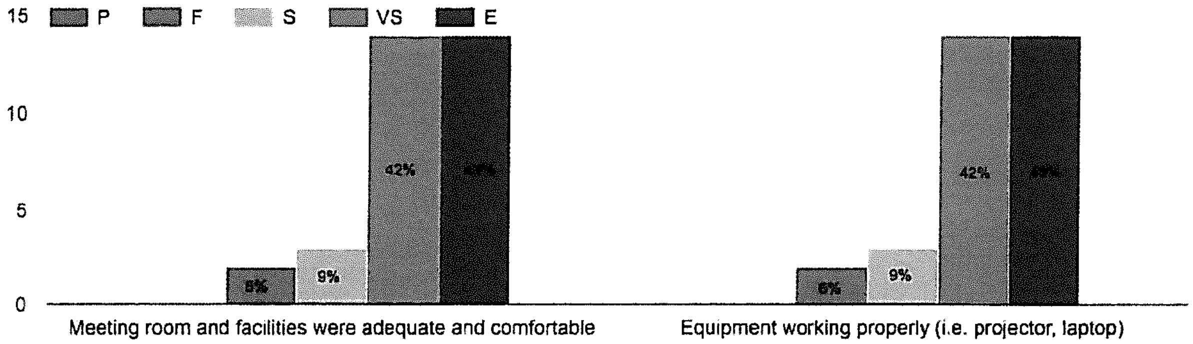
A total of 33 responses for the accommodation and venue and were categorized in two parts : the learning event venue and food. For the "learning event venue" 36% of the participants voted for excellent, 46% voted for very satisfactory, 12% voted for satisfactory and 6% voted for fair. On the "food" 36% of the participants voted for excellent, 46% voted for very satisfactory, 9% voted for satisfactory, 9% voted for fair and 1% voted for poor.

3.) Food



A total of 33 responses for the food and were categorized in four parts : the food quality, the food taste, the cleanliness, and the serving time. First, for the "food quality" 30% of the participants voted for excellent, 49% voted for very satisfactory, 12% voted for satisfactory and 9% voted for fair. Second, for the "food taste" 27% of the participants voted for excellent, 52% voted for very satisfactory, 12% voted for satisfactory and 9% voted for fair. Third, for the "cleanliness" 27% of the participants voted for excellent, 49% voted for very satisfactory, 15% voted for satisfactory and 9% voted for fair. Lastly, for the "serving time" 30% of the participants voted for excellent, 46% voted for very satisfactory, 15% voted for satisfactory and 9% voted for fair.

4.) Equipment and Facilities



A total of 33 responses for the equipment and facilities and were categorized in two parts : the meeting room and facilities were adequate and comfortable and equipment working properly. For the both parts "meeting room and facilities were adequate and comfortable" and "equipment working properly" 43% of the participants voted for excellent, 42% voted for very satisfactory, 9% voted for satisfactory and 6% voted for fair.

CYBERSECURITY CAMPAIGN PROGRAM
October 18-21, 2023
Harolds Evotel Timog Avenue, Quezon City

II. Technical Training

A. Introduction

In the context of network management, the **Computer Emergency Response Team (CERT)** plays a key role in helping organizations to protect and defend against cyber threats, vulnerabilities, and incidents. CERT typically operates as a centralized, dedicated team within an organization that is responsible for coordinating the response to and recovery from cyber incidents, as well as monitoring and analyzing the latest cyber threats and vulnerabilities.

Some of the specific tasks and responsibilities of CERT in network management may include:

a. **Identifying and responding to cyber incidents:** CERT monitors the organization's networks and systems for signs of cyber-attacks and coordinates the response to such incidents. This may involve isolating affected systems, restoring systems and data, and working with other teams and stakeholders to minimize the impact of the incident.
b. **Analyzing and mitigating vulnerabilities:** CERT monitors and analyzes the latest cyber threats and vulnerabilities, and provides guidance on how to mitigate or eliminate them. This may involve issuing alerts and advisories and coordinating with other organizations and agencies to develop and implement effective countermeasures.
c. **Developing and implementing cybersecurity policies and procedures:** CERT works with other teams and stakeholders to develop and implement policies and procedures for protecting against cyber threats. This may involve establishing standards and guidelines for secure network design and configuration, as well as developing and implementing security controls and protocols.
d. **Providing cybersecurity training and awareness:** CERT conducts training and awareness programs to help individuals and organizations understand and manage cyber risks. This may include developing and delivering educational materials and programs, as well as promoting best practices and guidelines for cybersecurity.

B. Objectives

The seminar aims to:

1. Understand the incident handling life cycle;
2. Demonstrate basic skills in incident handling and vulnerability assessment;
3. Define and work on policies and procedures, and identify pitfalls;
4. Understand the infrastructure required to operate a successful CERT;
5. Understand the environment which the individual and the team must operate in;
6. Demonstrate an understanding of important computer security concepts; and,
7. Discuss the history of the Internet and important security events.

C. Participants

A total of 101 participants, forty (40) participants attended the face-to-face technical training and 61 thru online. Face-to-face participants are composed of ICT Focals from regional offices and bureaus. Online participants are mixed participants from DENR central office, regional office, and bureaus.

D. Technical Training

The cybersecurity technical training started on October 19, 2023 with an introduction to the speakers led by Ms. Christine Apple B. Pre of the Department of Information and Communications Technology (DICT). Ms. Pre also gave a quick view on the topics of the speakers and acknowledged the presence of the participants. During the morning session, Mr. Alwell C. Mulsid discussed his topics followed by the discussion of the topics of Mr. Ned G. Serate and Mr. Zairo Shin F. Maniacop in the afternoon.

E. Lecture/Discussion (First Day)

TOPICS/DISCUSSION	RESOURCE SPEAKER
Cyber Threat Landscape ❖ Cyber incident response ➢ Most affected sectors ➢ Targeted asset/s ❖ Learning from threat landscape ➢ Compromised websites and systems ■ Common types ■ Attacker's objectives ■ Attack vector ■ Preparation and prevention measures ■ Best practices ➢ Malware and malicious files ■ Common types ■ Attacker's objectives ■ Attack vector ■ Preparation and prevention measures ■ Best practices ■ Recommendations to all government agencies and critical infrastructure organizations ➢ Data exfiltration, data leak, and data breach ■ Common types ■ Attacker's objectives ■ Attack vector ■ Preparation and prevention measures	**Alwell C. Mulsid** Information Technology Officer I Incident Response Section NCERT Division, DICT

■ Best practices ➢ Technical assistance related to cybersecurity ■ Common types ■ Attacker's objectives ■ Attack vector ■ Preparation and prevention measures ■ Best practices ➢ Brute Force ■ Common types ■ Attacker's objectives ■ Attack vector ■ Preparation and prevention measures ■ Best practices ➢ Servers networks and infrastructure attacks ■ Common types ■ Attacker's objectives ■ Attack vector ■ Preparation and prevention measures ■ Best practices ➢ Distributed Denial of Service (DDoS) ■ Common types ■ Attacker's objectives ■ Attack vector ■ Preparation and prevention measures ■ Best practices ➢ Email attacks ■ Common types ■ Attacker's objectives ■ Attack vector ■ Preparation and prevention measures ■ Best practices ❖ Cyber threat intel and monitoring **CERT Essentials** ❖ Introduction to CERT ➢ Definition and its purpose ❖ Why do organizations need a CERT ❖ Benefits of setting up a CERT ❖ Types of CERT ❖ Steps on setting up a CERT	**Alwell C. Mulsid** Information Technology Officer I Incident Response Section NCERT Division, DICT

Solutions and Capabilities: Build, Optimize, Secure and Comply ❖ Security and compliance ➢ Consolidation and Simplification ➢ Managed threat complete ➢ Wholistic application protection ➢ Outsourced coding ➢ Mobile app protection ➢ Remote and privileged access ➢ Cyber threat intelligence (CTI) ➢ Brand protection platform ➢ Identity lifecycle management ➢ Cloud infra best practices ➢ Cyber range ❖ On-premise based (deployed solutions) ➢ (NG) packet brokers and taps ➢ Data diode ➢ Packet and TraceCapture (portable) ➢ Network probe ❖ Gefura	**Ned G. Serate** Consulting Principal Gefura, Inc. Itraverse Solutions Inc.
Vulnerability Management and Ethical Hacking ❖ Traffic light protocol (TLP) ❖ Introduction to vulnerability ➢ Vulnerability assessment ➢ Penetration testing ➢ Attacker team security assessment ➢ Defender team security assessment ❖ Ethical Hacking ➢ Hacking ➢ Black hat hackers ➢ Gray hat hackers ➢ White hat hackers ➢ Things to comply in conducting ethical hacking ❖ Vulnerability Management ➢ Asset management ➢ Identifying vulnerabilities ■ Common vulnerabilities and exposures (CVE) ■ Vulnerabilities identification scanning tools ➢ Evaluating Vulnerabilities ■ Common vulnerability scoring system (CVSS) ■ CVSS calculator ■ CVSS ratings ➢ Threatening Vulnerabilities	**Zairo Shin F. Maniacop** Information Technology Officer I VAPT Section NCERT Division, DICT

■ Based on prioritization ■ Based on severity ■ Based on capacity ➢ Reporting Vulnerabilities ❖ Vulnerability assessment and penetration testing	**Zairo Shin F. Maniacop** Information Technology Officer I VAPT Section NCERT Division, DICT

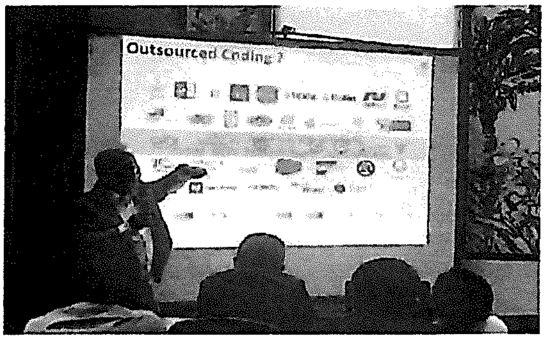
After the discussion of the last speaker, it was followed by the awarding of certificate, photo ops and closing remarks for day one administered by Mr. Eugene C. De Guzman of Knowledge and Information Systems Service - Network Infrastructure Management Division (KISS-NIMD) and Mr. Antonio S. Bautista Jr. of Knowledge and Information Systems Service - Information Systems Division (KISS-ISD).

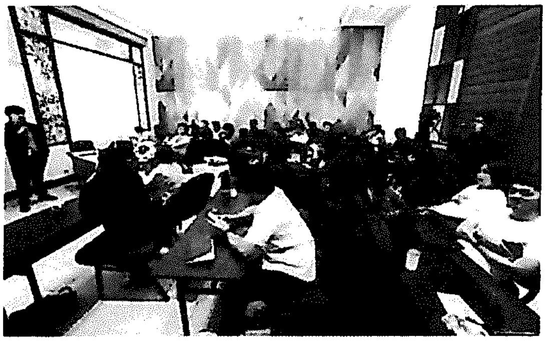
F. Lecture/Discussion (Second Day)

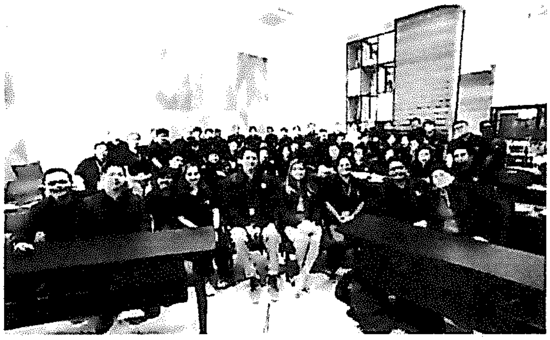
TOPICS/DISCUSSION	RESOURCE SPEAKER
Incident Handling and Management ❖ Incident response lifecycle (IRL) ➢ Prepare ➢ Identify ➢ Contain ➢ Analyze ➢ Eradicate ➢ Recover ➢ Lessons learned ❖ NIST cyber security framework (CSF) ➢ Incident management ➢ Communications strategy ➢ Communication methods ➢ Risk level of personal data breach ➢ Skills needed ❖ Incident Management ➢ Utilizing data	**Alwell C. Mulsid** Information Technology Officer I Incident Response Section NCERT Division, DICT

After the discussion of Mr. Mulsid on "Incident Handling and Management" the participants answered a post assessment and proceeded with a group activity entitled "Cybersecurity Tabletop Exercise" which was a discussion-based exercise conducted by injecting events in relation with the scenarios, and participants will discuss their roles and responses to solve the situation. The activity objective was to identify and evaluate the organizational cybersecurity knowledge of the participants and to share a collective knowledge on how to improve the prevention or response to security incidents in an organization. Participants were divided into 10 groups and each group solved six scenarios and shared their solutions to other groups. After solving three scenarios, Ms. Klarisse C. Angeles from Knowledge and Information Systems Service - Information Systems Division (KISS-ISD) shortly discussed the step-by-step guide on enabling Two-Factor Authentication (2FA) on Joomla admin page and thereafter, the morning session ended. The afternoon session is the continuation of the activity exercise and after that, the closing remarks and awarding of certificate to Mr. Alwell C. Mulsid led by Mr. Eugene C. De Guzman of KISS-NIMD.

G. Photo Documentation



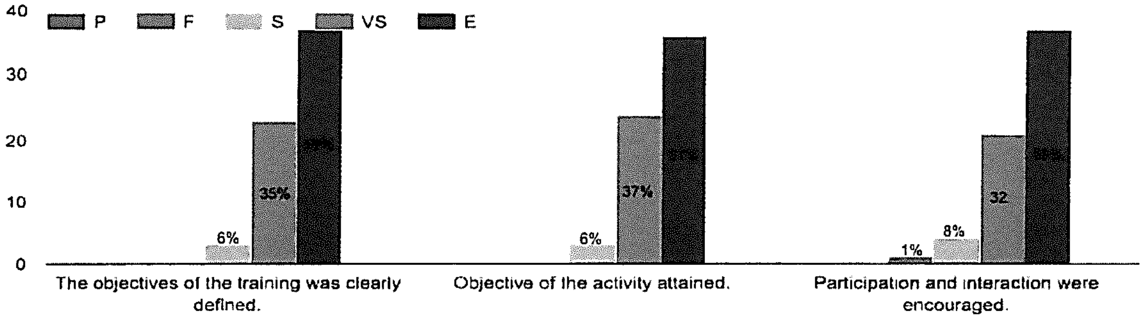




H. Evaluation Survey Result for the Technical Training dated October 18 - 21, 2023

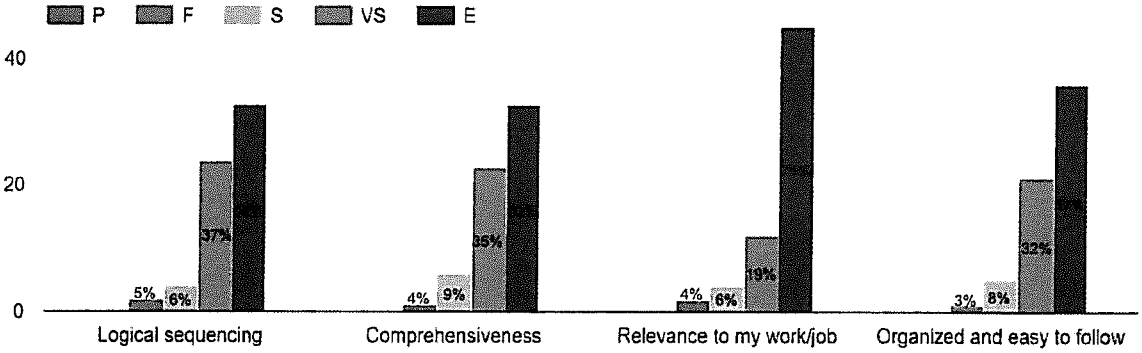
a. Substantive Matters

1.) OBJECTIVE OF THE EVENT



A total of 65 responses for the objective of the event and were categorized in three parts : the objectives of the training was clearly defined, the objective of the activity attained and the participation and interaction were encouraged. First, for the part of "objectives of the training was clearly defined", 59% of the participants voted for excellent, 35% voted for very satisfactory and 6% voted for satisfactory. Second for the part of "objective of the activity attained" 57% of the participants voted for excellent, 37% voted for very satisfactory and 6% voted for satisfactory. Lastly, for the "participation and interaction were encouraged" 59% of the participants voted for excellent, 32% voted for very satisfactory, 8% voted for satisfactory and 1% voted for fair.

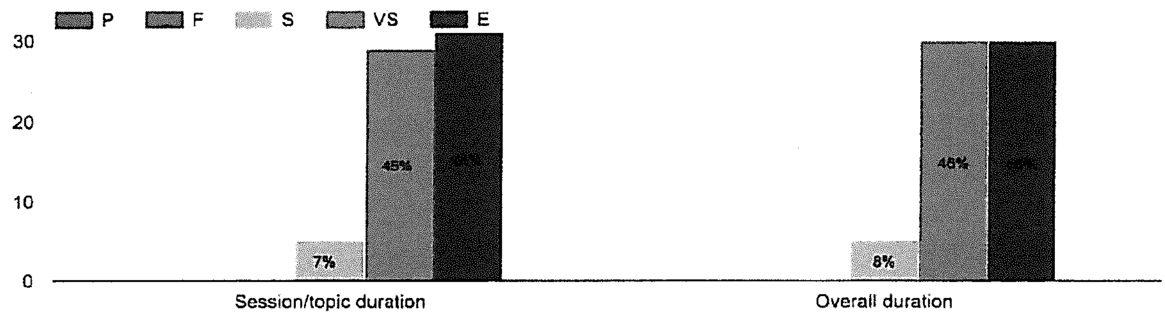
2.) TOPICS



A total of 65 responses for the topics and were categorized in four parts : the logical sequencing, the comprehensiveness, the relevance to my work/job, and the organized and easy to follow. First, for the part of logical sequencing, 52% of the participants voted for excellent, 37% voted for very satisfactory, 6% voted for satisfactory, and 5% voted for fair. Second, for the comprehensiveness 52% of the participants voted for excellent, 35% voted for very satisfactory, 9% voted for satisfactory, and 4% voted fair. Third, for the "relevance to my work/job", 71% of the participants voted for excellent, 19% voted for very satisfactory, 6% voted for satisfactory and 4% voted for fair. Lastly, for the "organized and easy to follow"

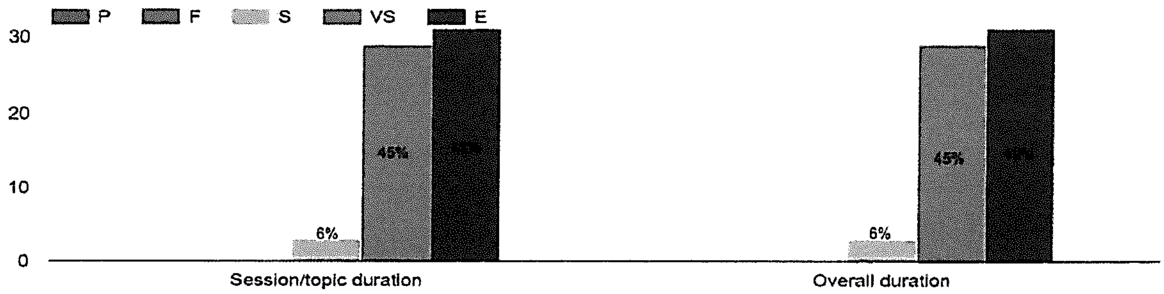
57% of the participants voted for excellent, 32% voted for very satisfactory, 8% voted for satisfactory and 3% voted for fair.

3.) TIME AND SCHEDULE



A total of 65 responses for the time and schedule and were categorized in two parts : the session/topic duration and the overall duration. For the "session/topic duration" 48% of the participants voted for excellent, 45% voted for very satisfactory and 7% voted for satisfactory. The "overall duration" 46% percent of the participants voted for excellent, 46% voted for satisfactory and 8% voted for satisfactory.

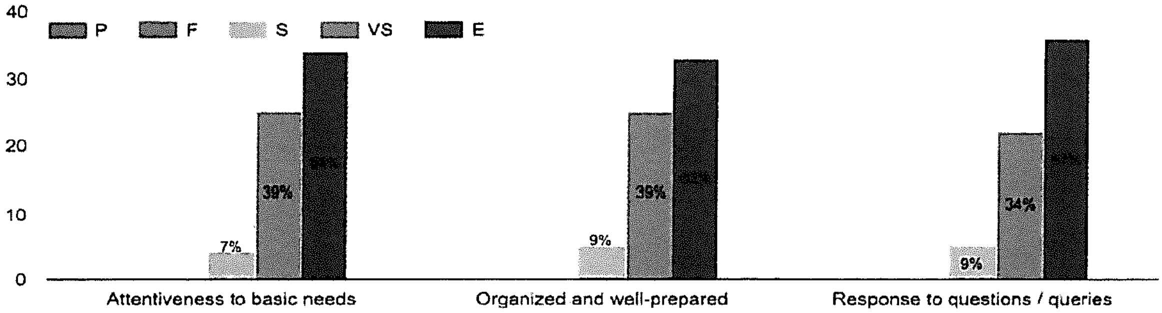
4.) METHODOLOGY



A total of 65 responses for the methodology and were categorized in two parts : the session/topic duration and the overall duration. For both parts 49% of the participants voted for excellent, 45% voted for very satisfactory and 6% voted for satisfactory.

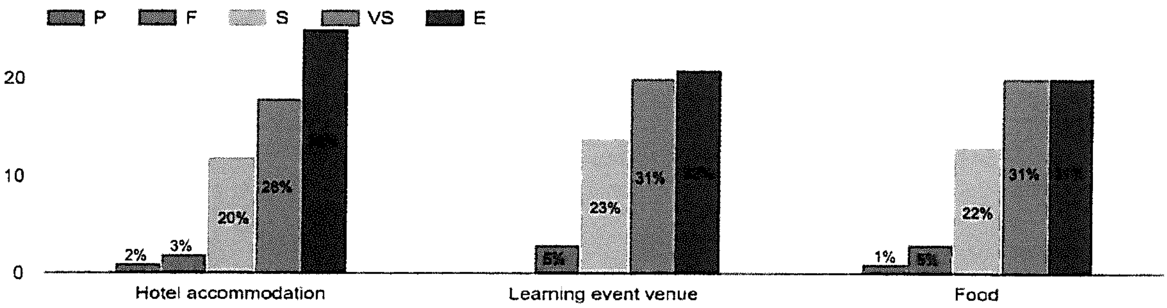
b. Administrative Matters

1.) Learning Event Team



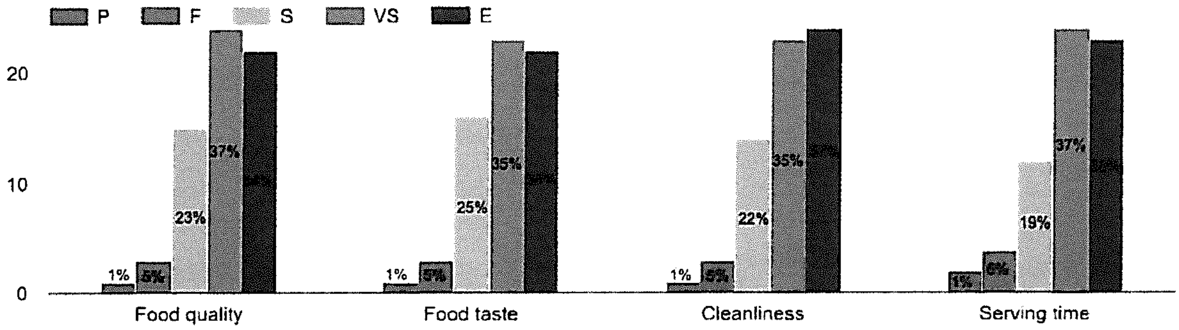
A total of 65 responses for the learning event team and were categorized in three parts : the attentiveness to basic need, the organized and well-prepared and the response to questions/queries. First, for the "attentiveness to basics needs" 54% of the participants voted for excellent, 39% voted for very satisfactory and 7% voted for satisfactory. Second, for the "organized and well prepared" 52% of the participants voted for excellent, 39% voted for very satisfactory and 9% voted for satisfactory. Lastly, for the "response to questions/queries" 57% of the participants voted for excellent, 34% voted for very satisfactory and 9% voted for satisfactory.

2.) Accommodation and Venue



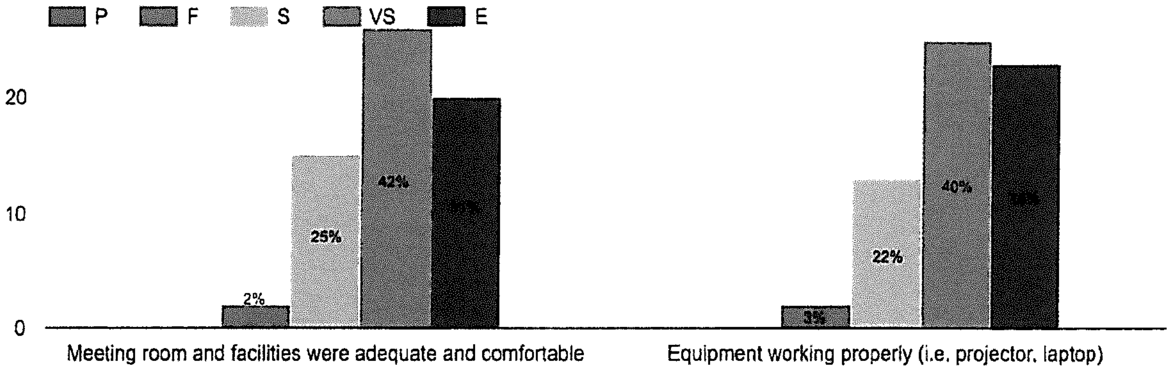
A total of 65 responses for the accommodation and venue and were categorized in three parts : the hotel accommodation, the learning event venue and food. First, for the "hotel and accommodation" 39% of the participants voted for excellent, 28% voted for very satisfactory, 20% voted satisfactory, 3% voted for 2% voted for fair. Second, for the "learning event venue" 32% of the participants voted for excellent, 31% voted for very satisfactory, 23% voted for satisfactory and 5% voted for fair. Lastly, for the "food" 31% of the participants voted for excellent, 31% voted for very satisfactory, 22% voted for satisfactory, 5% voted for fair and 1% voted for poor.

3.) Food



A total of 65 responses for the food and were categorized in four parts : the food quality, the food taste, the cleanliness, and the serving time. First, for the "food quality" 34% of the participants voted for excellent, 37% voted for very satisfactory, 23% voted for satisfactory, 5% voted for fair and 1% voted for poor. Second, for the "food taste" 34% of the participants voted for excellent, 35% voted for very satisfactory, 25% voted for satisfactory, 5% voted for fair and 1% voted for poor. Third, for the "cleanliness" 37% of the participants voted for excellent, 35% voted for very satisfactory, 22% voted for satisfactory, 5% voted for fair and 1% voted for poor. Lastly, for the "serving time" 35% of the participants voted for excellent, 37% voted for very satisfactory, 19% voted for satisfactory, 6% voted for fair and 3% voted for poor.

4.) Equipment and Facilities



A total of 65 responses for the equipment and facilities and were categorized in two parts : the meeting room and facilities were adequate and comfortable and equipment working properly. For the "meeting room and facilities were adequate and comfortable" 31% of the participants voted for excellent, 42% voted for very satisfactory, 25% voted for satisfactory and 2% voted for fair. On "equipment working properly" 35% of the participants voted for excellent, 40% voted for very satisfactory, 22% voted for satisfactory and 3% voted for fair.

Prepared by:

Mary Joy P. Yumol
Administrative Assistant III

Hannah Joyce R. Español
Information Officer

nzmatias
Nizethal Aducal-Matias
OIC Chief, Network Infrastructure
Management Division

Noted by:

ARomasanta
Arlene A. Romasanta
Director, Knowledge and Information
Systems Service